procedures, appropriate to the different file types, to compare their resistance to noise with our NCD results.

REFERENCES

[1] Yale Face Database [Online]. Available: http://cvc.yale.edu/projects/yalefaces/yalefaces.html

[2] C. Bennett, P. Gacs, M. Li, P. Vitanyi, and W. Zurek, "Information distance," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1407–1423, Jul. 1998.

[3] R. Cilibrasi, A. L. Cruz, and S. de Rooijet, The CompLearn Toolkit [Online]. Available: http://www.complearn.org software available at

[4] R. Cilibrasi and P. Vitanyi, "Clustering by compression," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1523–1545, Apr. 2005.

[5] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[6] M. Hart, The Gutemberb Project [Online]. Available: http://www.gutenberg.org free electronic books available at

[7] M. Li, X. Chen, X. Li, B. Ma, and P. Vitányi, "The similarity metric," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3250–3264, Dec. 2004.

[8] M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*. New York: Springer-Verlag, 1997.

Optimal Encoding of Classical Information in a Quantum Medium

Noam Elron and Yonina C. Eldar, *Member, IEEE*

***Abstract*—We investigate optimal encoding and retrieval of digital data, when the storage/communication medium is described by quantum mechanics. We assume an m-ary alphabet with arbitrary prior distribution, and an n-dimensional quantum system. Under these constraints, we seek an encoding–retrieval setup, comprised of code-states and a quantum measurement, which maximizes the probability of correct detection. In our development, we consider two cases. In the first, the measurement is predefined and we seek the optimal code-states. In the second, optimization is performed on both the code-states and the measurement. We show that one cannot outperform "pseudo-classical transmission," in which we transmit n symbols with orthogonal code-states, and discard the remaining symbols. However, such pseudo-classical transmission is not the only optimum. We fully characterize the collection of optimal setups, and briefly discuss the links between our findings and applications such as quantum key distribution and quantum computing.**

***Index Terms*—Bilinear matrix inequality, quantum detection, quantum key distribution, semidefinite programming, transmitter design.**

I. INTRODUCTION

Underlying any scheme for the storage or transmission of information is a physical medium. The encoding and the retrieval of information must therefore involve considerations as to the nature of the medium, with regard to possible corruption of the retrieved data, due to interaction with the environment or to physical limitations of the medium itself. This work is concerned with the encoding of digital information in media, whose physics is described by the laws of quantum mechanics [1].

We concentrate on digital information with a finite alphabet, i.e., the data is one of m possible messages, each one associated with a prior probability p_i. Retrieval of the data is done by performing a measurement, thereby detecting the state of the system.

In classical models of communication channels (e.g., the additive white Gaussian noise (AGWN) channel), much effort has been made to find optimal constellations, i.e., a set of signals and a detector, which minimize the detection error [2], [3]. The aim of this correspondence is to do the same for a quantum model of a communications link.

The state of a quantum system is mathematically represented by a unit trace positive semidefinite operator ρ on an n-dimensional Hilbert space $\mathcal{H}$. Encoding digital information in a quantum system is done by preparing the system in one of m predefined states $\{\rho_i\}_{i=1}^m$, each associated with one of the possible messages.

Retrieval is achieved by performing a quantum measurement, and determining in which of these predetermined states the system has been prepared. The outcome of a measurement is random, i.e., a quantum encoding–retrieval setup is characterized by transition probabilities

$$\Pr\{i\,|\,j\} \triangleq \Pr\{\text{out} = \text{symbol } i\,|\,\text{in} = \text{symbol } j\}.$$

This is reminiscent of the more common classical setups, but whereas the randomness there is induced by noise from the environment, in the quantum model, the randomness is inherent in the system itself. In the general case, no quantum measurement can determine without fail which of the states is present; there is a nonzero probability of detection error, i.e., $\Pr\{i\,|\,j\} > 0$ for $i \neq j$. The question is then, what collection of code-states $\{\rho_i\}$ and valid quantum measurement would yield favorable performance. A popular measure of performance is the probability of correct detection

$$P_d = \sum_{i=1}^{m} p_i \Pr\{i\,|\,i\}.$$

The focus of this correspondence is the design of a complete digital communications channel (or memory unit), in which the designer can choose both the code-states ρ_i and the detection measurement. We assume that the nature of the data, which is designated by the number of possible symbols m and their prior probabilities p_i, is known. We also assume that the dimension n of the quantum system is given. The dimension of the quantum system determines the ability of the medium to transmit (or store) data reliably, much like the signal-to-noise ratio in classical systems.

Thus, we seek the optimal setup, comprised of code-states and a measurement that maximize P_d under a constraint of the dimension n of the system. We find the maximum attainable value of P_d for data with an arbitrary prior distribution, and completely characterize the optimal setups, which achieve this value of P_d.

When the number of symbols m is no larger than the dimension of the Hilbert space n, one can simply choose ρ_i as orthogonal pure states and attain perfect detection. When $m > n$, this is no longer possible, and quantum encoding becomes nontrivial.

Motivation for using many symbols in a quantum system of low dimension may stem from benefits, which a protocol provides, for which one is willing to sacrifice the probability of detection or the information rate. For instance, in protocols of quantum key distribution [4], the use of many states enables the detection of eavesdropping on the communication. In Section V-C we elaborate on this point.

Manuscript received January 2, 2006; revised January 4, 2007.

N. Elron was with the Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel. He is now with Neocraft Ltd., Ramat-Gan 52573, Israel (e-mail: noam.elron@neocraft.com).

Y. C. Eldar is with the Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: yonina@ee.technion.ac.il).

Communicated by A. Winter, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2006.894686

This problem also has relevance for quantum computation in practical situations. Assume one wishes to conduct a computation which has a number of outputs m, but due to technological or budget limitations, cannot realize enough qubits such that the dimension of the system is large enough. The possible outputs cannot be encoded using the "computational basis" vectors, since there are not enough of them. By applying our results, a quantum algorithm can be designed, such that the probability of error in the outcome is small.

The problem of distinguishing among a collection of *specified* quantum states, i.e., when the code-states ρ_i are a given, is regularly referred to as *quantum detection* or *quantum state discrimination*, and has been studied in detail. Necessary and sufficient conditions for an optimal measurement, which maximizes the probability of correct detection P_d, have been derived [5]–[7]. Explicit solutions to the problem are known in some particular cases [8]–[12], including ensembles obeying a large class of symmetries [13]. The optimal measurement can also be calculated numerically, to within arbitrary accuracy, and in polynomial complexity [7].

Several alternative approaches have also been investigated. These include optimization with regard to other performance criteria, such as mutual information [5] or the worst case posterior probability [14]. Another approach is *unambiguous detection* [15]–[17] in which one allows for an inconclusive result but does not allow for error. More recently, interest has grown in detection in a noisy environment [18]–[20], and in situations where the states are only partially known [21] or the prior probabilities not specified [22].

In Section II, the problem is presented in more detail. Then, in Section III, we show that the optimal code-states for a predetermined measurement are states which lie in the eigenspaces of the measurement operators associated with the maximal eigenvalues. This result is of interest both in its own right, and as part of the design of complete optimal encoding–retrieval setups.

Sections IV and V are the heart of this work. In Section IV, we show that when encoding digital information in a quantum system of dimension n, the maximum attainable probability of correct detection may be achieved by simply discarding $m-n$ of the symbols and using an orthonormal set to encode the remaining n symbols with perfect reconstruction. We dub this method *pseudo-classical* transmission. This is, however, not the only possible encoding–retrieval setup which achieves the maximal value of P_d. In Section V, we show that all setups that attain the maximum are composed of pure code-states and of rank-1 measurement operators, and fully characterize the collection of optimal setups. The importance of finding all the optimal setups is discussed in Subsection V-C, where we outline possible use of our results in the analysis of quantum communication and computation protocols.

II. Problem Formulation

A. Notation

According to the postulates of quantum mechanics [1], a physical system is mathematically represented by an n-dimensional complex Hilbert space $\mathcal{H}$. The state of the system ρ is represented by a positive semidefinite (PSD) Hermitian operator on $\mathcal{H}$, such that $\mathrm{Tr}(\rho)=1$. Throughout, we shall use the notation $A\geq 0$ to indicate that an operator A is PSD, and the notation $A\geq B$ to imply that $A-B$ is PSD. If $\mathrm{rank}(\rho)=1$, then it is known as a pure state.

As is customary in work relating to quantum theory, we shall use Dirac's notation of linear algebra, wherein a vector is denoted by $|u\rangle$, its Hermitian conjugate by $\langle u|$, and inner and outer products are signified by $\langle u\,|\,v\rangle$ and $|u\rangle\langle v|$, respectively. We do not assume that $|u\rangle$ is normalized. We denote by $\mathcal{R}(A)$ the range space of a Hermitian operator A, and by $\mathcal{M}(A)$ the eigenspace of its maximal eigenvalue.

B. Encoding Data in Quantum Media

We wish to encode digital information in a quantum medium. The information is represented by an m-ary alphabet, where each symbol has a prior probability p_i. Without loss of generality, we assume that the prior distribution obeys $p_1\geq p_2\geq\cdots\geq p_m>0$. The encoding is achieved by associating with each symbol a predefined quantum state ρ_i, and preparing the system in the appropriate state. We shall refer to the states ρ_i as *code-states*. To a set of code-states $\{\rho_i\}_{i=1}^m$ we refer as an *ensemble*.

Retrieval of the information is accomplished by using a positive operator valued measurement (POVM), which is a set of m operators $\Pi=\{\Pi_i\}_{i=1}^m$, which satisfy

$$\Pi_i\geq 0,\qquad 1\leq i\leq m$$
$$\sum_{i=1}^m\Pi_i=I.$$

This is the most general type of measurement allowed by the laws of quantum physics.

The measurement results in one of m possible outcomes, where, given that the state of the system is ρ, the probability of the ith outcome is

$$\Pr\{i\}=\mathrm{Tr}(\Pi_i\rho).$$

Thus, the probability of correctly detecting the encoded message is

$$P_d(\{\Pi_i\},\{\rho_i\})=\sum_{i=1}^m p_i\mathrm{Tr}(\Pi_i\rho_i).$$

We use P_d as the criterion for measuring the quality of an encoding–retrieval setup.

In the next section, we find the optimal code-states, in the sense of maximal P_d, for a given measurement. We then characterize, in Sections IV and V, all optimal encoding–retrieval setups, when the design specifications are the nature of the data (the prior probabilities p_i), and the dimension n of the quantum system.

III. Designing Code-States for an Arbitrary Measurement

In this section, we answer the following question. If the detector, i.e., the measurement Π, and the prior probabilities of the data p_i are predetermined, what would be a good choice of code-states ρ_i to encode the data in a quantum medium of dimension n, in terms of P_d? This question is of interest, due to possible implementation restrictions on the detector. As indicated in the introduction, the reverse situation, that of designing a measurement to discriminate among arbitrary states, has been thoroughly studied.

Our result is stated formally in Theorem 1.

Theorem 1: Let $\{p_i\}_{i=1}^m$ be a probability distribution, and let $\{\Pi_i\}_{i=1}^m$ be the measurement operators of a detector. An ensemble of quantum states $\{\rho_i\}_{i=1}^m$ maximizes P_d if and only if

$$\mathcal{R}(\rho_i)\subseteq\mathcal{M}(\Pi_i).$$

Denoting the maximal eigenvalue of Π_i as $\sigma_{\Pi_i}^{\max}$, the maximal probability of correct detection is given by

$$P_d^{\mathrm{opt}}=\sum_{i=1}^m p_i\sigma_{\Pi_i}^{\max}.$$

Note that for all i such that $\Pi_i = 0$, one has that $\mathcal{M}(\Pi) = \mathcal{H}$, and any choice of ρ_i is optimal.

Proof: The optimal states $\hat{\rho}_i$ are a solution to

$$\max_{\rho_i} \sum_{i=1}^{m} p_i \operatorname{Tr}(\Pi_i \rho_i) \quad \text{s.t.} \begin{cases} \rho_i \geq 0 \\ \operatorname{Tr}(\rho_i) = 1. \end{cases} \tag{1}$$

The objective function in (1) is additive in the variables ρ_i, and the constraints on each of the ρ_i are independent. Hence, (1) is separable in i, i.e., the states $\hat{\rho}_i$ are optimal if and only if they are also the solutions to m problems of the form (one for each i)

$$\max_{\rho} \operatorname{Tr}(\Pi \rho) \quad \text{s.t.} \begin{cases} \rho \geq 0 \\ \operatorname{Tr}(\rho) = 1. \end{cases} \tag{2}$$

Any quantum state ρ, such that $\rho \geq 0$ and $\operatorname{Tr}(\rho) = 1$, has an eigendecomposition of the form

$$\rho = \sum_{j=1}^{n} g_j |u_j\rangle\langle u_j|,$$

where $g_j \geq 0, \sum_{j=1}^{n} g_j = 1$, and $\langle u_j \mid u_j \rangle = 1$. Since $\Pi \geq 0$, we have that

$$\begin{aligned} \operatorname{Tr}(\Pi\rho) &= \sum_{j=1}^{n} g_j \langle u_j|\Pi|u_j\rangle \\ &\leq \langle \hat{u}|\Pi|\hat{u}\rangle \sum_{j=1}^{n} g_j \\ &= \langle \hat{u}|\Pi|\hat{u}\rangle \\ &\leq \sigma_{\Pi}^{\max} \end{aligned}$$

where $\langle \hat{u}|\Pi|\hat{u}\rangle = \max_j \langle u_j|\Pi|u_j\rangle$ and $\sigma_{\Pi}^{\max}$ is the largest eigenvalue of Π. If $\Pi = 0$, then the upper bound is zero and any $\rho \geq 0$ is optimal. When $\Pi \neq 0$, equality is achieved if $\operatorname{Tr}(\Pi\rho) = \sigma_{\Pi}^{\max}$, i.e., *only* when ρ lies in the eigenspace corresponding to $\sigma_{\Pi}^{\max}$. □

Note that the optimal code-states $\hat{\rho}_i$ are independent of each other and of the prior probabilities p_i. Also, note that the optima (the solutions of the problem (1)) form a convex set.

Corollary 1.1: If for all $i, \dim\mathcal{M}(\Pi_i) = 1$, then the ensemble which maximizes P_d is unique.

Proof: When $\dim\mathcal{M}(\Pi_i) = 1$ then ρ_i must be the pure state which spans $\mathcal{M}(\Pi_i)$, which is unique (due to the requirement of normalization). If this is true for all i, then the entire set of code-states is unique. □

In applications, one may have the freedom to choose which symbol will be detected by which of the detection operators. Recalling that, we assumed the prior probabilities p_i to be sorted in descending order, maximal P_d can be attained when the detection operators are sorted such that $\sigma_{\Pi_1}^{\max} \geq \sigma_{\Pi_2}^{\max} \geq \cdots \geq \sigma_{\Pi_m}^{\max}$. Doing this, and selecting the optimal code-states as above, will lead to the maximal value of $P_d = \sum_i p_i \sigma_{\Pi_i}^{\max}$.

IV. Optimal Quantum Encoding

We now find the maximal attainable value of P_d when encoding data in a quantum medium. We assume that the nature of the data itself, which is manifested in the prior probabilities p_i, is predetermined, and so is the quantum system itself (i.e., the dimension n). We aim to find an encoding–retrieval setup that maximizes P_d.

Thus, our goal is to find the solutions to

$$\max_{\Pi_i, \rho_i} \sum_{i=1}^{m} p_i \operatorname{Tr}(\Pi_i \rho_i) \quad \text{s.t.} \begin{cases} \rho_i \geq 0, & \operatorname{Tr}(\rho_i) = 1 \\ \Pi_i \geq 0, & \sum_{i=1}^{m} \Pi_i = I. \end{cases} \tag{3}$$

This optimization problem is of a class known as *Bilinear Matrix Inequality* (BMI) problems [23]. BMIs are nonconvex, and in general, finding a global optimum is an NP-hard problem [24]. Nonetheless, for this particular BMI (3), we are able to formulate a closed-form solution, and to completely specify the optimal set.

When the dimension n of the quantum system is equal to the number of possible messages m, then perfect retrieval ($P_d = 1$) is achievable by choosing the code-states ρ_i to be mutually orthogonal pure states, and the measurement such that $\Pi_i = \rho_i$. When $n < m$, this is no longer possible. The most straightforward approach to quantum encoding when $n < m$ is to simply disregard $m - n$ of the messages and aim to perfectly retrieve the remaining n messages. It is clear that the smallest probability of error will occur if the disregarded messages are the ones with smallest prior probabilities. Thus, this approach is embodied in the ensemble–detector setup

$$\Pi_i = \begin{cases} |u_i\rangle\langle u_i|, & 1 \leq i \leq n \\ 0, & n < i \leq m \end{cases} \qquad \rho_i = \begin{cases} |u_i\rangle\langle u_i|, & 1 \leq i \leq n \\ \text{don't care}, & n < i \leq m \end{cases} \tag{4}$$

where $\{|u_i\rangle\}_{i=1}^{n}$ is some orthonormal system. When using this setup $P_d = \sum_{i=1}^{n} p_i$.

The distinction between classical and quantum systems is very strongly linked to the fact that nonorthogonality between two quantum states affects the ability to distinguish between them. There is no classical analogue of this property. When the states that a quantum system may be in are mutually orthogonal, it is said to be in "the classical limit." The fact that the setup (4) is comprised only of pure mutually orthogonal states implies that it is classical in nature and that the losses encountered are not due to the fact that the system is governed by quantum mechanics, but to a lossy preprocessing (disregarding some of the messages). In the sequel, we refer to (4) as *pseudo-classical* transmission.

It would, at first glance, seem that one may somehow be able to utilize the "quantumness" of the system, i.e., nonorthogonal code-states and measurements, in order to improve the probability of correct detection P_d. We now formulate and prove a theorem which shows this to be impossible.

Theorem 2: Let $\{p_i\}_{i=1}^{m}$ be a probability distribution with $p_1 \geq p_2 \geq \cdots \geq p_m < 0$. Denoting by $\hat{P}_d$ the maximal probability of correct detection for a quantum system of dimension $n \leq m$, we have that

$$\hat{P}_d = \sum_{i=1}^{n} p_i.$$

Proof: Let $\tilde{P}_d = \sum_{i=1}^{n} p_i$. Since the pseudo-classical setup (4) achieves $P_d(\{\Pi_i\}, \{\rho_i\}) = \tilde{P}_d$, we have that $\hat{P}_d \geq \tilde{P}_d$. We prove the theorem by showing that $\hat{P}_d \leq \tilde{P}_d$.

The maximal value of P_d is the solution of (3). From Theorem 1, after maximizing with respect to ρ_i, (3) reduces to

$$\max_{\Pi_i} \sum_{i=1}^{m} p_i \sigma_{\Pi_i}^{\max} \quad \text{s.t.} \begin{cases} \Pi_i \geq 0 & \text{(a)} \\ \sum_{i=1}^{m} \Pi_i = I. & \text{(b)} \end{cases} \tag{5}$$

The constraint (5a) implies that

$$\sigma_{\Pi_i}^{\max} \geq 0, \qquad 1 \leq i \leq m \tag{6}$$

and from (5b)

$$\sigma_{\Pi_i}^{\max} \leq 1, \qquad 1 \leq i \leq m$$
$$\sum_{i=1}^{m} \sigma_{\Pi_i}^{\max} \leq n. \tag{7}$$

(The bottom expression in (7) is obtained by taking the trace of (5b)). We now replace (5) by a scalar program

$$\max_{\sigma_i} \sum_{i=1}^{m} p_i \sigma_i \quad \text{s.t.} \begin{cases} 0 \leq \sigma_i \leq 1 \\ \sum_{i=1}^{m} \sigma_i \leq n. \end{cases} \tag{8}$$

Problem (8) was created by relaxing the constraints of problem (5)—we keep only the constraints on the eigenvalues and disregard the original matrix–inequality constraints. Therefore, the solution of (8) is always larger or equal to the solution of (5), and thus, serves as an upper bound.

The optimization problem (8) is a linear program. Its *Lagrange dual* [25] is given by

$$\min_{\eta_i, \nu_i, \mu} g(\eta_i, \mu) \quad \text{s.t.} \begin{cases} \eta_i, \nu_i, \mu \geq 0 & \text{(a)} \\ p_i - \eta_i + \nu_i - \mu = 0 & \text{(b)} \end{cases} \tag{9}$$

where $1 \leq i \leq m$ and

$$g(\eta_i, \mu) = \sum_{i=1}^{m} \eta_i + n\mu.$$

Using the constraint (9b), the variables ν_i can be eliminated, yielding

$$\min_{\eta_i, \mu} g(\eta_i, \mu) \quad \text{s.t.} \begin{cases} \eta_i, \mu \geq 0 & \text{(a)} \\ \eta_i + \mu \geq p_i. & \text{(b)} \end{cases} \tag{10}$$

From Lagrange duality theory, for any point in the feasibility set of (10), the objective $g(\eta_i, \mu)$ is greater or equal to the solution of the primal problem (8). In other words, for any dual feasible point (η, μ), $g(\eta_i, \mu)$ is an upper bound on the solution of (5). Consider

$$\hat{\eta}_i = \begin{cases} p_i - p_{n+1}, & 1 \leq i \leq n \\ 0, & n < i \leq m \end{cases}$$
$$\hat{\mu} = p_{n+1}. \tag{11}$$

Because $p_1 \geq \cdots \geq p_m$ it is dual feasible. For this choice

$$g(\hat{\eta}_i, \hat{\mu}) = \sum_{i=1}^{m} \hat{\eta}_i + n\hat{\mu} = \sum_{i=1}^{n} (\hat{\eta}_i + \hat{\mu}) = \sum_{i=1}^{n} p_i.$$

In conclusion, we have shown that

$$\max(3) = \max(5) \leq \max(8) \leq \min(10) \leq \sum_{i=1}^{n} p_i$$

which implies that for any valid ensemble and detector

$$P_d = \sum_{i=1}^{m} p_i \operatorname{Tr}(\Pi_i \rho_i) \leq \tilde{P}_d. \qquad \square$$

The implication of Theorem 2 is that one can achieve the optimal probability of correct detection by using orthogonal pure states and von Neumann measurements, which are easy to implement. Nevertheless, there may be setups $\{\rho_i, \Pi_i\}_{i=1}^{m}$ other then (4) which attain $P_d(\{\Pi_i\}, \{\rho_i\}) = \hat{P}_d$. In the next section, we identify all the ensemble–detector setups which achieve maximum probability of correct detection. The importance of characterizing the set of optima is that we may be able to select an optimum that has preferable performance with regard to other quality of service measures. Also, there may be communication protocols which require using a "nonclassical" ensemble. These aspects are discussed in greater detail in Section V-C.

V. Characterization of Optimal Setups

In this section, we introduce the notion of *tight frame encoding setups*, and show that all optima are of this form (Theorem 3). We then fully characterize the set of optima for a given prior probability distribution (Theorem 4 and corollaries).

A. Tight Frame Encoding Setups

A *tight frame* [26] is a set of m vectors $\{|u_i\rangle\}_{i=1}^{m}$ which satisfy

$$\sum_{i=1}^{m} |u_i\rangle\langle u_i| = I. \tag{12}$$

We define a "Tight Frame Encoding Setup" (TFES) to be an ensemble–detector setup of the form

$$\Pi_i = |u_i\rangle\langle u_i|,$$
$$\rho_i = \begin{cases} \frac{1}{\langle u_i \mid u_i \rangle} |u_i\rangle\langle u_i|, & \langle u_i \mid u_i \rangle > 0 \\ \text{don't care}, & \langle u_i \mid u_i \rangle = 0 \end{cases}$$

where the vectors $|u_i\rangle$ obey (12). The pseudo-classical setup (4) is an example of a TFES. The probability of correct detection when using a TFES is $P_d = \sum_{i=1}^{m} p_i \langle u_i \mid u_i \rangle$.

The constraint (12) on the vectors ensures that Π is a valid POVM. It also implies several properties of the vectors $|u_i\rangle$, which are summarized in the following lemma.

Lemma 1: Let $\{|u_i\rangle\}_{i=1}^{m}$ be a set of vectors which satisfy (12). Then

$$\langle u_i \mid u_i \rangle \leq 1 \tag{13}$$
$$\text{if } \langle u_i \mid u_i \rangle = 1 \text{ then } \langle u_i \mid u_j \rangle = \delta_{i,j} \tag{14}$$
$$\sum_{i=1}^{m} \langle u_i \mid u_i \rangle = n. \tag{15}$$

Proof: Can be found in many texts on tight frames, e.g., [27], [28]. □

Tight frames are of interest in many fields and applications where one seeks a set of vectors whose mutual "interference" is minimal. Specifically, in classical communication, they play an important role in syncronous code-division multiple-access (CDMA) systems [29], [30]. Also, the simplex constellation, which is known to be optimal under certain energy constraints [2], is a tight frame.

The significance of TFESs to quantum encoding is established by the following result.

Theorem 3: All ensemble–detector setups $\{\hat{\rho}_i, \hat{\Pi}_i\}_{i=1}^m$ which achieve $P_d(\{\hat{\Pi}_i\}, \{\hat{\rho}_i\}) = \hat{P}_d$ are TFESs.

The proof of Theorem 3, relies on the following lemma, whose proof is given in the Appendix.

Lemma 2: For any ensemble–detector setup $(\hat{\rho}_i, \hat{\Pi}_i)$ which achieves $P_d(\{\hat{\Pi}_i\}, \{\hat{\rho}_i\}) = \hat{P}_d$, the largest eigenvalues of the detection operators satisfy

$$\sum_{i=1}^{m} \sigma_{\hat{\Pi}_i}^{\max} = n.$$

Proof (of Theorem 3): For any POVM, we have that

$$\mathrm{Tr}(\Pi_i) \geq \sigma_{\Pi_i}^{\max} \tag{16}$$

$$\sum_{i=1}^{m} \mathrm{Tr}(\Pi_i) = n \tag{17}$$

where (17) comes from taking the trace of the requirement $\sum_{i=1}^m \hat{\Pi}_i = I$.

Assume that an ensemble–detector setup $\{\hat{\rho}_i, \hat{\Pi}_i\}$ achieves $\hat{P}_d$. Using (17) with Lemma 2, we get that

$$\sum_{i=1}^{m} \mathrm{Tr}(\hat{\Pi}_i) = \sum_{i=1}^{m} \sigma_{\hat{\Pi}_i}^{\max}$$

which, in conjunction with (16), shows that for any such detector

$$\mathrm{Tr}(\hat{\Pi}_i) = \sigma_{\hat{\Pi}_i}^{\max}, \qquad 1 \leq i \leq m$$

This in turn implies that

$$\mathrm{rank}(\hat{\Pi}_i) \leq 1, \qquad 1 \leq i \leq m$$

i.e., the detection elements of any detector which is part of an optimal setup are of the form $\hat{\Pi}_i = |u_i\rangle\langle u_i|$ (where $|u_i\rangle$ may also be the null vector). In order for $\hat{\Pi}$ to be a valid POVM, the set of vectors $\{|u_i\rangle\}_{i=1}^m$ must obey (12).

Since $\{\hat{\rho}_i, \hat{\Pi}_i\}$ is assumed to be an optimal setup, then $\hat{\rho}_i$ must be an optimal ensemble for the detector $\hat{\Pi}$. Thus, from Theorem 1 we have that for any i, such that $\langle u_i \,|\, u_i\rangle > 0$

$$\hat{\rho}_i = \frac{1}{\langle u_i \,|\, u_i\rangle} |u_i\rangle\langle u_i|.$$

If $\langle u_i \,|\, u_i\rangle = 0$, then $\hat{\rho}_i$ can be any quantum state. □

An interesting aspect of the above result is that $\hat{P}_d$ can only be attained by setups in which the detected code-states (those for which the corresponding measurement operator is not zero) are pure states. This is hardly surprising, since obviously, for mixed states the chances of "interference" between code-states are greater.

B. Choice of TFES

From Theorem 3 we know that all optima are TFESs. Not all choices of TFES are, however, necessarily optimal. We now show that the set of optimal TFESs is dependent on the prior probabilities $\{p_i\}_{i=1}^m$, and on the dimension of the quantum medium n, and characterize this dependence. The following results (Theorem 4 and corollaries) fully characterize all optimal solutions for a given prior distribution and dimension n.

In order to formulate our results, we introduce a classification of the symbols into three distinct subsets, according to the prior probability distribution and the dimension n. Recalling that we assume $p_1 \geq p_2 \geq \cdots \geq p_m$, we define

- $\mathcal{I}_1 = \{i \,|\, p_i > p_n\}$,
- $\mathcal{I}_2 = \{i \,|\, p_i = p_n\}$,
- $\mathcal{I}_3 = \{i \,|\, p_i < p_n\}$.

Note that $\mathcal{I}_1$ and $\mathcal{I}_3$ may be empty.

Theorem 4: Let $\{p_i\}_{i=1}^m$ be a nonincreasing distribution of probabilities, and let $\{|u_i\rangle\}_{i=1}^m$ be the vectors of a TFES in a quantum system of dimension n. This TFES is optimal in the sense of probability of correct detection if and only if i) for all $i \in \mathcal{I}_1, \langle u_i \,|\, u_i\rangle = 1$, and ii) for all $i \in \mathcal{I}_3, \langle u_i \,|\, u_i\rangle = 0$.

Before proving Theorem 4, we point out the following important corollaries.

Corollary 4.1: Let $\{p_i\}_{i=1}^m$ be a nonincreasing distribution of probabilities, and let $\{\hat{\rho}_i, \hat{\Pi}_i\}_{i=1}^m$ be an *optimal* encoding setup in a quantum system of dimension n. Then

1) $\Pr\{j \,|\, i\} = \delta_{i,j}, \qquad i \in \mathcal{I}_1$,
2) $\Pr\{\mathrm{detect}\ i\} = 0, \quad i \in \mathcal{I}_3$.

Proof: From Theorem 3, we know that the ensemble–detector setup is a TFES. From Theorem 4, for all $i \in \mathcal{I}_1, \hat{\Pi}_i = |u_i\rangle\langle u_i|$, such that $\langle u_i \,|\, u_i\rangle = 1$. Together with (14), it is easy to see that

$$\Pr\{j \,|\, i\} = \mathrm{Tr}(\hat{\Pi}_j \hat{\rho}_i) = \frac{1}{\langle u_i \,|\, u_i\rangle} |\langle u_i \,|\, u_j\rangle|^2 = \delta_{i,j}.$$

Also from Theorem 4, for all $i \in \mathcal{I}_3, \hat{\Pi}_i = 0$, indicating that the probability of detecting the ith message is $\Pr\{\mathrm{detect}\ i\} = \sum_j p_j \mathrm{Tr}(\hat{\Pi}_i \hat{\rho}_j) = 0$. □

Corollary 4.2: Let $\{p_i\}_{i=1}^m$ be a nonincreasing distribution of probabilities. If $p_n > p_{n+1}$ then any optimal setup $\{\hat{\rho}_i, \hat{\Pi}_i\}_{i=1}^m$ must be of the form (4) (pseudo-classical).

Proof: From Theorem 3, the optimal setup must be a TFES. When $p_n > p_{n+1}$, we have $\mathcal{I}_3 = \{n+1, \ldots, m\}$, which, using Theorem 4, indicates that

$$\langle u_i \,|\, u_i\rangle = 0, \qquad n+1 \leq i \leq m.$$

Together with (12) this implies

$$\sum_{i=1}^{n} |u_i\rangle\langle u_i| = I. \tag{18}$$

A set of n vectors in n-dimensional space can satisfy (18) if and only if they form an orthonormal set. Thus, the only optimal setup when $p_n > p_{n+1}$ is (4). □

Corollary 4.3: If $p_i = \frac{1}{m}$ for all i, then all TFESs achieve $\hat{P}_d$.

Proof: The Corollary follows directly from Theorem 4, for $\mathcal{I}_1 = \mathcal{I}_3 = \emptyset$. □

We now prove Theorem 4.

Proof (of Theorem 4): Assume that $\{|u_i\rangle\}_{i=1}^m$ are the vectors of a TFES which is optimal in the sense of P_d. Assume that $\mathcal{I}_1 \neq \emptyset$ and denote by k the largest index in $\mathcal{I}_1$ (i.e., $\mathcal{I}_1 = \{1, \ldots, k\}$). This means that $p_k > p_{k+1} = p_{k+2} = \cdots = p_n$ (from the definition of $\mathcal{I}_1$, we have that $k < n$). For any TFES we can write

$$\begin{aligned} P_d &= \sum_{i=1}^{m} p_i \langle u_i \,|\, u_i \rangle \\ &= \sum_{i=1}^{k} p_i \langle u_i \,|\, u_i \rangle + \sum_{i=k+1}^{m} p_i \langle u_i \,|\, u_i \rangle \\ &\leq \sum_{i=1}^{k} p_i \langle u_i \,|\, u_i \rangle + p_{k+1} \sum_{i=k+1}^{m} \langle u_i \,|\, u_i \rangle \qquad (19) \\ &= \sum_{i=1}^{k} p_i \langle u_i \,|\, u_i \rangle + p_{k+1} \left(n - \sum_{i=1}^{k} \langle u_i \,|\, u_i \rangle \right) \qquad (20) \\ &= \sum_{i=1}^{k} [p_i \langle u_i \,|\, u_i \rangle + p_{k+1}(1 - \langle u_i \,|\, u_i \rangle)] + (n-k) p_{k+1} \qquad (21) \end{aligned}$$

where the transition from (19) to (21) relies on (15).

Recall that for all $i \in \mathcal{I}_1$ we have $p_i > p_{k+1}$. If for some $1 \leq i \leq k, \langle u_i \,|\, u_i \rangle < 1$, then from (21)

$$\begin{aligned} P_d &< \sum_{i=1}^{k} [p_i \langle u_i \,|\, u_i \rangle + p_i (1 - \langle u_i \,|\, u_i \rangle)] + (n-k) p_{k+1} \\ &= \sum_{i=1}^{k} p_i + (n-k) p_{k+1} = \sum_{i=1}^{n} p_i = \hat{P}_d. \end{aligned}$$

Here we have relied on the fact that $p_{k+1} = p_{k+2} = \cdots = p_n$. Therefore, in order to achieve $\hat{P}_d$, the vectors $|u_i\rangle$ must satisfy

$$\langle u_i \,|\, u_i \rangle = 1, \qquad i \in \mathcal{I}_1.$$

This concludes the proof of the first statement of the "only if" direction.

We go on to prove the second statement. Assume that $k' = \max \mathcal{I}_2 < m$ (i.e., $\mathcal{I}_3 = \{k'+1, \ldots, m\} \neq \emptyset$). By definition $p_{k'} > p_{k'+1}$. We again have

$$P_d = \sum_{i=1}^{m} p_i \langle u_i \,|\, u_i \rangle = \sum_{i=1}^{k'} p_i \langle u_i \,|\, u_i \rangle + \sum_{i=k'+1}^{m} p_i \langle u_i \,|\, u_i \rangle.$$

If for some $i \in \mathcal{I}_3, \langle u_i \,|\, u_i \rangle > 0$, then

$$\begin{aligned} P_d &< \sum_{i=1}^{k'} p_i \langle u_i \,|\, u_i \rangle + p_{k'} \sum_{i=k'+1}^{m} \langle u_i \,|\, u_i \rangle \qquad (22) \\ &= \sum_{i=1}^{n} p_i \langle u_i \,|\, u_i \rangle + p_n \sum_{i=n+1}^{m} \langle u_i \,|\, u_i \rangle \qquad (23) \\ &= \sum_{i=1}^{n} p_i \langle u_i \,|\, u_i \rangle + p_n \left(n - \sum_{i=1}^{n} \langle u_i \,|\, u_i \rangle \right) \qquad (24) \\ &= \sum_{i=1}^{n} p_i \langle u_i \,|\, u_i \rangle + p_n \sum_{i=1}^{n} (1 - \langle u_i \,|\, u_i \rangle) \\ &\leq \sum_{i=1}^{n} p_i \langle u_i \,|\, u_i \rangle + \sum_{i=1}^{n} p_i (1 - \langle u_i \,|\, u_i \rangle) \\ &= \sum_{i=1}^{n} p_i = \hat{P}_d \end{aligned}$$

where the transitions from (22) to (24) rely on the fact that $k' \in \mathcal{I}_2$ and on (15). Thus, for any TFES which achieves maximal P_d

$$\langle u_i \,|\, u_i \rangle = 0, \qquad i \in \mathcal{I}_3.$$

We continue by proving the "if" direction. Assume that for all $i \in \mathcal{I}_1, \langle u_i \,|\, u_i \rangle = 1$, and that for all $i \in \mathcal{I}_3, \langle u_i \,|\, u_i \rangle = 0$. We must first note that under these conditions, using (15) yields

$$\sum_{i=1}^{k'} \langle u_i \,|\, u_i \rangle = n. \qquad (25)$$

If $\mathcal{I}_1 = \emptyset$, then $\mathcal{I}_2 = \{1, \ldots, k'\}$. We can then write

$$\begin{aligned} P_d &= \sum_{i=1}^{m} p_i \langle u_i \,|\, u_i \rangle \qquad (26) \\ &= p_1 \sum_{i=1}^{k'} \langle u_i \,|\, u_i \rangle \qquad (27) \\ &= n p_1 = \sum_{i=1}^{n} p_i = \hat{P}_d \qquad (28) \end{aligned}$$

where the transition from (26) to (27) relies on the facts that for all $i > k', \langle u_i \,|\, u_i \rangle = 0$ and $p_1 = p_2 = \cdots = p_n$. The transition from (27) to (28) is based on (25).

If $\mathcal{I}_1 = \{1, \ldots, k\}$ and $\mathcal{I}_2 = \{k+1, \ldots, k'\}$ then similarly

$$\begin{aligned} P_d &= \sum_{i=1}^{m} p_i \langle u_i \,|\, u_i \rangle \\ &= \sum_{i=1}^{k} p_i \langle u_i \,|\, u_i \rangle + p_{k+1} \sum_{i=k+1}^{k'} \langle u_i \,|\, u_i \rangle \\ &= \sum_{i=1}^{k} p_i + (n-k) p_{k+1} = \sum_{i=1}^{n} p_i = \hat{P}_d \end{aligned}$$

thereby completing the proof. □

Theorem 5, below, summarizes the assertions of Theorems 2, 3, and 4, in concise form, and completely characterizes all optimal transmitter–receiver setups.

Theorem 5: Let $\{p_i\}_{i=1}^m$ be a probability distribution with $p_1 \geq p_2 \geq \cdots \geq p_m > 0$. For a given number $n \leq m$, define the index sets

- $\mathcal{I}_1 = \{i \,|\, p_i > p_n\}$,
- $\mathcal{I}_2 = \{i \,|\, p_i = p_n\}$,
- $\mathcal{I}_3 = \{i \,|\, p_i < p_n\}$.

The maximal probability of correct detection for a quantum system of dimension $n \leq m$ is

$$\hat{P}_d = \sum_{i=1}^{n} p_i.$$

The optimum is achieved if and only if the ensemble–detector setup is of the form

$$\begin{aligned} \Pi_i &= |u_i\rangle\langle u_i| \\ \rho_i &= \begin{cases} \frac{1}{\langle u_i \,|\, u_i \rangle} |u_i\rangle\langle u_i|, & \langle u_i \,|\, u_i \rangle > 0 \\ \text{don't care}, & \langle u_i \,|\, u_i \rangle = 0 \end{cases} \end{aligned}$$

where the vectors $\{|u_i\rangle\}_{i=1}^m$ obey

$$\begin{aligned} \sum_{i=1}^{m} |u_i\rangle\langle u_i| &= I \\ \langle u_i \,|\, u_i \rangle &= 1, \qquad i \in \mathcal{I}_1 \\ \langle u_i \,|\, u_i \rangle &= 0, \qquad i \in \mathcal{I}_3. \end{aligned}$$

Put in words, maximum P_d can only be attained by a TFES, where the messages with high prior probabilities ($i \in \mathcal{I}_1$) are encoded using

orthogonal code states, and are thus recovered perfectly (Corollary 4.1), and the messages with low prior probabilities ($i \in \mathcal{I}_3$) are discarded—much like in pseudo-classical encoding. In choosing the remaining frame vectors, one has freedom and they can be chosen to be nonorthogonal. Important special cases are when $p_{n+1} > p_n$, where one has no freedom and the only optimum is pseudo-classical encoding (Corollary 4.2), and the equiprobable case $p_i = \frac{1}{m}$, where there is complete freedom in choosing the TFES frame vectors (Corollary 4.3).

C. Application to the Analysis of Communication Protocols

In many applications, additional constraints, other than the ones imposed by physics, are placed on the encoding-retrieval setup. In quantum key distribution (QKD) [4], for example, constraints arise due to the need for security against eavesdropping. Further constraints may occur due to technical (implementation) issues. Our results can then serve two purposes. The first is to quantify the degradation in P_d due to the need to meet the extra design constraints. This can be done by simply comparing the performance of the constrained system to the theoretical upper bound $\hat{P}_d$. The second possible use of this work, in this context, is to search within the set of optimal TFESs for a setup, which is close to meeting the demands posed by the application. When taking the latter approach we are assured optimal performance with regard to P_d.

As an example, consider the BB84 protocol [31]. In this QKD protocol, Alice wishes to send Bob secure binary information. In order to counter possible eavesdropping, she sends one of $m = 4$ messages with $p_i = \frac{1}{4}$ over a two-dimensional quantum channel. The code-states used are denoted $|u_{ij}\rangle$, where $i, j = 0, 1$, and they obey the relations

$$|\langle u_{ij} \mid u_{i'j'}\rangle|^2 = \begin{cases} \delta_{j,j'}, & i = i' \\ 1/2, & i \neq i' \end{cases}$$

$$\frac{1}{2}\sum_{i,j=0}^{1} |u_{ij}\rangle\langle u_{ij}| = I. \tag{29}$$

Note that (29) indicates that this collection of vectors is a tight frame.

Bob utilizes the POVM (of order 4) $\Pi_{ij} = \frac{1}{2}\langle u_{ij} \mid u_{ij}\rangle$, in order to retrieve Alice's message. They then exchange knowledge on which "pair of states" was received (by, for example, comparing the i index). If both the sent and the detected symbols originate from the same pair, then the transferred bit of information is taken as the member of the pair that was detected (the j index). If the symbols originate from different pairs, then the received symbol is discarded. In order to promote security, Alice and Bob use $m > n$, at a cost of reduced data rate. The security of this protocol has been extensively studied (e.g., [32]).

The probability of correct detection achieved by Bob prior to the exchange of the i index is $P_d = 1/2$. This is equal to the upper bound $\hat{P}_d$ for this case, meaning that under the requirement of countering eavesdropping, Bob achieves the maximal possible performance. The fact that the upper bound is reached is hardly surprising in the context of a protocol as simple as BB84. It does, however, serve to illustrate the possible use of the unconstrained upper bound $\hat{P}_d$ in quantifying the efficacy of more complex communication protocols.

VI. Conclusion

We have addressed the question of retrieval of digital data encoded in a quantum medium, using as our main performance criterion the probability of correct detection. We have found the optimal code-states for an arbitrary detector, and the optimal encoding–retrieval setups for an arbitrary prior distribution.

In terms of P_d, one cannot do better than pseudo-classical transmission (orthonormal code-states and measurement operators). We have, however, indicated that under certain circumstances, there are benefits for using fully quantum setups (nonorthogonal code-states).

The natural extension of this work is the design of optimal setups with added constraints. Such constraints may arise due to requirements other than reliable communication, such as the need for security discussed above. Constraints may also stem from implementation issues which are typical to specific quantum systems that regularly serve for transmission and storage of information.

Appendix
Proof of Lemma 2

Assume that $(\bar{\eta}_i, \bar{\mu})$ is a feasible point of the program (10), such that $\bar{\mu} = 0$. From the constraint (10b), $\bar{\eta}_i$ must satisfy $\bar{\eta}_i \geq p_i$ and then

$$g(\bar{\eta}_i, \bar{\mu}) \geq \sum_{i=1}^{m} p_i > \sum_{i=1}^{n} p_i = g(\hat{\eta}_i, \hat{\mu})$$

where $(\hat{\eta}_i, \hat{\mu})$ are defined in (11). Thus, $(\bar{\eta}_i, \bar{\mu})$ cannot be a dual optimal point. All dual optimal points must satisfy $\mu \neq 0$.

One of the Karush–Kuhn–Tucker (KKT) conditions for the solution to problem (8) is

$$\mu\left(n - \sum_{i=1}^{m} \sigma_i\right) = 0.$$

Since the dual optimal $\mu \neq 0$, then any optimal values of σ_i must satisfy

$$\sum_{i=1}^{m} \sigma_i = n. \tag{A1}$$

Let $\{\Pi_i\}$ be a POVM, which is part of an optimal ensemble–detector setup, i.e., $\sum_i p_i \sigma_{\Pi_i}^{\max} = \hat{P}_d$. By choosing

$$\hat{\sigma}_i = \sigma_{\Pi_i}^{\max} \tag{A2}$$

we get $\sum_i p_i \hat{\sigma}_i = \hat{P}_d$, ensuring that $\hat{\sigma}_i$ are an optimum of (8), and thus satisfy (A1). In conjunction with (A2), this proves the lemma.

Acknowledgment

We would like to thank Moshe Nazarathy, who helped spark our interest in the subjects of this correspondence. We also benefited from discussions with Oded Regev and Tal Mor.

References

[1] A. Peres, *Quantum Theory: Concepts and Methods*. Waterloo, ON, Canada: Kluwer Academic, 1993.

[2] A. V. Balakrishnan, "A contribution to the sphere-packing problem of communication systems," *J. Math. Anal. Appl.*, vol. 3, pp. 485–506, Dec. 1961.

[3] M. Steiner, "The strong simplex conjecture is false," *IEEE Trans. Inf. Theory*, vol. 40, no. 3, pp. 721–731, May 1994.

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Jan. 2002.

[5] A. S. Holevo, "Statistical decision theory for quantum systems," *J. Multivar. Anal.*, vol. 3, pp. 337–394, Dec. 1973.

[6] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 2, pp. 125–134, Mar. 1975.
[7] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Designing optimal quantum detectors via semidefinite programming," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1007–1012, Apr. 2003.
[8] C. W. Helstrom, *Quantum Detection and Estimation Theory*. New York: Academic, 1976.
[9] M. Charbit, C. Bendjaballah, and C. W. Helstrom, "Cutoff rate for the m-ary psk modulation channel with optimal quantum detection," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1131–1133, Sep. 1989.
[10] M. Osaki, M. Ban, and O. Hirota, "Derivation and physical interpretation of the optimum detection operators for coherent-state signals," *Phys. Rev. A*, vol. 54, pp. 1691–1701, Aug. 1996.
[11] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation," *Int. J. Theor. Phys.*, vol. 36, pp. 1269–1288, 1997.
[12] Y. C. Eldar and G. D. Forney Jr., "On quantum detection and the square-root measurement," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 858–872, Mar. 2001.
[13] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Optimal detection of symmetric mixed quantum states," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1198–1207, Jun. 2004.
[14] R. L. Kosut, I. Walmsley, Y. C. Eldar, and H. Rabitz, Quantum State Detector Design: Optimal Worst-Case a Posteriori Performance, [Online]. Available: http://arXiv.org/abs/quant-ph/0403150, 2004, submitted for publication.
[15] I. D. Ivanovic, "How to differentiate between nonorthogonal states," *Phys. Lett. A*, vol. 123, pp. 257–259, Aug. 1987.
[16] Y. C. Eldar, "A semidefinite programming approach to optimal unambiguous discrimination of quantum states," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 446–456, Feb. 2003.
[17] Y. C. Eldar, M. Stojnic, and B. Hassibi, "Optimal quantum detectors for unambiguous detection of mixed states," *Phys. Rev. A*, vol. 69, no. 6, p. 062318, 2004.
[18] M. Sasaki, R. Momose, and O. Hirota, "Quantum detection for on-off keyed mixed-state signals with a small amount of thermal noise," *Phys. Rev. A.*, vol. 55, no. 4, pp. 3222–3225, Apr. 1997.
[19] V. Vilnrotter and C. W. Lau, Quantum Detection of Binary and Ternary Signals in the Presence of Thermal Noise Fields, NASA, The InterPlanetary Network Progr. Rep. 42-152, Oct.-Dec. 2002, Feb. 2003 [Online]. Available: http://ipnpr.jpl.nasa.gov/tmo/progress_report/42-152/152B.pdf
[20] J. I. Concha and H. V. Poor, "Multiaccess quantum channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 725–747, May 2004.
[21] N. Elron and Y. C. Eldar, "Quantum detection with uncertain states," *Phys. Rev. A.* vol. 72, p. 032338, 2005.
[22] G. M. D'Ariano, M. F. Sacchi, and J. Kahn, "Minimax quantum state discrimination," *Phys. Rev. A.* 2005 [Online]. Available: http://arXiv.org/abs/quant-ph/0504048
[23] Y. Xiao, F. Crusca, and E. K.-W. Chu, Bilinear Matrix Inequalities in Robust Control: Phase I—Problem Formulation Monash Univ., Victoria, Australia, Tech. Rep. MECSE-3-1996, Apr. 1996 [Online]. Available: http://www.ds.eng.monash.edu.au/techrep/reports/
[24] O. Toker and H. Özbay, "On the $\mathcal{NP}$-hardness of solving bilinear matrix inequalities and simultaneous stabilization with static output feedback," in *Proc. 1995 American Control Conf.*, Seattle, WA, 1995, pp. 2525–2526.
[25] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, Mar. 2004.
[26] Y. C. Eldar and G. D. Forney, Jr., "Optimal tight frames and quantum measurement," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 599–610, Mar. 2002.
[27] O. Christensen, *An Introduction to Frames and Riesz Bases*. Boston, MA: Birkhäuser, 2003.
[28] P. G. Casazza, M. Fickus, J. Kovačević, M. T. Leon, and J. C. Tremain, "A physical interpretation of finite tight frames," in *Harmonic Analysis and Applications*, C. Heil, Ed. Boston, MA: Birkhäuser, 2006.
[29] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
[30] P. Viswanath, V. Anantharam, and D. N. C. Tse, "Optimal sequences, power control, and user capacity of syncronous CDMA systems with linear MMSE multiuser receivers," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1968–1983, Sep. 1999.
[31] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, Dec. 1984, pp. 175–179.
[32] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul. 2000.

A Generalized Bose-Chowla Family of Optical Orthogonal Codes and Distinct Difference Sets

Oscar Moreno, *Fellow, IEEE*, Reza Omrani, *Member, IEEE*, P. Vijay Kumar, *Fellow, IEEE*, and Hsiao-feng (Francis) Lu, *Member, IEEE*

***Abstract*—A new construction of optical orthogonal codes is provided in this correspondence which is a generalization of the well-known construction of distinct difference set (DDS) by Bose and Chowla. This construction is optimal with respect to the Johnson bound and has parameters $n = q^a - 1, \omega = q,$ and $\lambda = 1$.**

***Index Terms*—Distinct difference set (DDS), optical code-division multiple access (OCDMA), optical orthogonal code (OOC), optical CDMA.**

I. Introduction

Recently, there has been an upsurge of interest in applying code-division multiple access (CDMA) techniques to optical networks (see, for example, [1]–[4]). Part of the revived interest in optical CDMA is on account of the inherent added security, flexibility, and simplicity of network control that CDMA provides [5].

An (n, ω, λ) optical orthogonal code (OOC) $\mathcal{C}$ where $1 \leq \lambda \leq \omega \leq n$ is a family of $\{0, 1\}$-sequences of length n and Hamming weight ω satisfying

$$\sum_{k=0}^{n-1} x(k)y(k \oplus_n \tau) \leq \lambda \tag{1}$$

whenever either $x \neq y$ or $\tau \neq 0$, where by $\oplus_n$ we mean addition modulo n. We will refer to λ as the maximum correlation parameter.

Manuscript received March 1, 2004; revised November 22, 2006. This work was supported in part by the National Science Foundation under CISE Grant EIA-0080926, the National Science Foundation under Grant NSF-ITR CCR-0326628, by DARPA under OCDMA Program Grant N66001-02-1-8939, the Taiwan National Science Council under Grant NSC 95-2219-E-194-011, and the DRDO-IISc Program on Advanced Research in Mathematical Engineering. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Yokohama, Japan, June/July 2003.

O. Moreno is with the Department of Computer Science, University of Puerto Rico, Rio Piedras, PR 00931 (e-mail: moreno@uprr.pr).

R. Omrani and P. V. Kumar are with the Electrical Engineerng-Systems, University of Southern California, Los Angeles, CA 90089 USA (e-mail: omrani@usc.edu;vijayk@usc.edu).

H.-f. Lu is with the Department of Communication Engineering, National Chung-Cheng University, Min-Hsiung, Chia-Yi, 621 Taiwan, R.O.C. (e-mail: francis@ccu.edu.tw).

Communicated by G. Zémor, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2007.894658