Optimal reconstruction systems for erasures and for the q-potential[☆]

Pedro G. Massey

Depto. Matemática, FCE, UNLP and Instituto Argentino de Matemática, CONICET, Argentina

A R T I C L E   I N F O

A B S T R A C T

In this paper we introduce the q-potential as an extension of the Benedetto–Fickus frame potential, defined on general reconstruction systems and show that protocols are the minimizers of this potential under certain restrictions. We extend recent results of B.G. Bodmann on the structure of optimal protocols with respect to 1 and 2 lost packets where the worst (normalized) reconstruction error is computed with respect to a compatible unitarily invariant norm. We finally describe necessary and sufficient (spectral) conditions, that we call q-fundamental inequalities, for the existence of protocols with prescribed properties by relating this problem to Klyachko's and Fulton's theory on sums of hermitian operators.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

Signal transmission through a noisy channel typically uses the following strategy: a generic signal is decomposed (encoded) into a sequence of coefficients which are then grouped into a number of packets of the same size. Then these packets are sent through the noisy channel. For practical purposes, we shall assume that the noise in the channel can not affect the integrity of the data in each packet; we can think that these *small* pieces of data are protected by an efficient error-correcting algorithm. Still, the noise of the channel may cause the loss of some packets so that the reconstruction of the signal is done possibly without the whole set of packets. Hence we search for encoding–decoding schemes that minimize, with respect to some measure, the worst case error between (a normalization of) the original signal and the reconstructed signal for a fixed number of packet losses, under certain hierarchies (see the beginning of Section 4 for a description of these hierarchies). This and similar problems have been

---

considered recently by Casazza and Kovacevic [13], Holmes and Paulsen [19], Bodmann and Paulsen [8], Bodmann [6], Bodmann, Paulsen and Kribs [7] and Strohmer and Heath [32], where they describe the structure of optimal encoding–decoding schemes based on a particular choice to measure the worst case reconstruction error. In the present paper we extend some of the results obtained in those works, as we show that the previously mentioned optimal schemes are actually optimal with respect to a continuous family of measures of the worst case reconstruction error in the more general setting of block-encoding–decoding introduced in [6]. Our approach and techniques related with these problems are derived here as a generalization of those in [6].

The optimal schemes found in the frame-based transmission model (under suitable restrictions) are related with the so-called Parseval (or more generally tight) frames. There is a natural generalization of Parseval frames introduced by Bodmann in [6], the so-called *protocols*, which is the starting point for the development of the theory of optimal protocols under packet-erasures in that paper. In this setting, the optimal protocols correspond to some *projective* protocols, which were originally introduced by Casazza and Kutyniok [14] under the name of (Parseval) frames of subspaces, and recently have also been called Fusion frames [15]. But there are more general *reconstruction systems* (see Defintion 3.1) than protocols, just as there are more general frames than Parseval frames.

In order to investigate possible advantages of general protocols in the class of reconstruction systems we introduce what we called the q-potential, which is a generalization of the frame potential defined by Benedetto and Fickus in [4] and further considered in [10,11]. In our case the q-potential of a reconstruction system takes values in the cone of positive matrices, rather than numerical values, a fact that makes it difficult to compare q-potentials of different systems. Still, we show that under suitable conditions, protocols are the minimizers of the q-potential within reconstruction systems with respect to (*sub*)*majorization* and thus we obtain lower bounds and minimizers of a family of (anti)entropic measures of the q-potential. These results indicate that protocols are indeed a good starting point for the theory of block-erasures.

On the other hand, although there are interesting techniques to construct 2-uniform protocols, i.e., protocols that are optimal for two packet losses (see [6,8,19]), the problem of finding necessary and sufficient conditions for the existence of protocols that are optimal for one packet loss has been considered open (see the discussion in [7]). We relate this problem to a problem solved by Klyachko [24] and Fulton [18] related with Horn's conjecture on the sums of hermitian matrices and hence we obtain a characterization of the existence of such optimal protocols. This result can be regarded as an extension of the equivalence of the Schur–Horn problem on the main diagonal of a hermitian operator with prescribed spectrum and the problem of finding necessary and sufficient conditions for the existence of a frame for a finite dimensional Hilbert space with prescribed norms and frame operator as described in [2] (see also [12,26,33]), using the notion of extended majorization as described in [28]. We then derive the q-fundamental inequalities (see Corollary 5.3), that is a generalization of the fundamental inequality found in [11].

The paper is organized as follows. After some preliminary facts in Section 2, we introduce in Section 3 the q-potential defined on the class of reconstruction systems and show that the protocols are the minimizers of this positive operator function with respect to submajorization. Thus, it is natural to restrict the analysis of optimal reconstruction systems for erasures to protocols. In Section 4.1 we give a complete description of optimal protocols for one packet loss, when we base the measure of the worst case reconstruction error on a compatible unitarily invariant norm. In Section 4.2 we deal with the case of two lost packets where we show explicitly a family of optimal protocols, when restricted to a certain family of optimal protocols for one loss packet. We then show that this restriction is automatically satisfied by optimal frames for one coefficient loss and obtain a generalization of previous results on the structure of optimal frames for two lost packets. Finally, in Section 5 we consider the problem of designing protocols with prescribed additional properties.

2. Preliminaries

In this note we shall denote by $\mathcal{H} = \mathbb{F}^d$ and $\mathcal{K} = \mathbb{F}^l$, where $\mathbb{F}$ stands for $\mathbb{R}$ or $\mathbb{C}$ and $l \leqslant d$. Hence, if $l < d$ there is a natural injection $\iota : \mathcal{K} \rightarrow \mathcal{H}$ such that $\iota(x) = (x, 0_{d-l})$, where 0_{d-l} denotes the zero

vector in $\mathbb{R}^{d-l}$. Moreover, $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}'$ under the identification given by ι, for $\mathcal{K}' = \iota(K)^\perp$. In what follows, given $r, t \in \mathbb{N}$ we denote by $M_{r,t}(\mathbb{F})$ the $\mathbb{F}$-algebra of all $r \times t$ matrices with entries in $\mathbb{F}$. For simplicity we note $M_r(\mathbb{F})$ instead of $M_{r,r}(\mathbb{F})$. We further consider $M_r(\mathbb{F})^{sa}, M_r(\mathbb{F})^+$ and $\mathcal{U}(r)$ that are the real space of self-adjoint matrices, the cone of positive semi-definite matrices and the group of unitary matrices over $\mathbb{F}$, respectively. If $A \in M_d(\mathbb{C})^{sa}$ then we denote by $\lambda(A) \in \mathbb{R}^d$ the vector of eigenvalues of A (counting multiplicities) with its entries arranged in decreasing order. The canonical basis of $\mathcal{H} = \mathbb{F}^d$ is denoted $\{e_i\}_{i=1}^d$. By fixing the canonical basis in $\mathcal{H}$ and $\mathcal{K}$ respectively, we shall identify $\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{K})$ and $\mathcal{L}(\mathcal{H}, \mathcal{K})$ with $M_d(\mathbb{F}), M_l(\mathbb{F})$ and $M_{l,d}(\mathbb{F})$ respectively. The vector $\mathbf{e}_d \in \mathbb{R}^d$ is the vector with all its entries equal to 1. Finally, if X is a finite set then $|X|$ denotes its cardinal.

2.1. Submajorization in $M_l(\mathbb{C})^{sa}$

Given $x \in \mathbb{R}^l$ we denote by $x^\downarrow \in \mathbb{R}^l$ the vector obtained by re-arrangement of the coordinates of x in non-increasing order. Given $x, y \in \mathbb{R}^l$ we say that x is *submajorized* by y, and write $x \prec_w y$ if

$$\sum_{i=1}^k x_i^\downarrow \leqslant \sum_{i=1}^k y_i^\downarrow, \quad \text{for } 1 \leqslant k \leqslant l. \tag{1}$$

If we further have that $\text{tr}(x) := \sum_{i=1}^l x_i = \sum_{i=1}^l y_i$ then we say that x is *majorized* by y, and write $x \prec y$.

Example 2.1. As an elementary example, that we shall use repeatedly in what follows, let $x \in \mathbb{R}_{\geqslant 0}^l$ and $0 \leqslant a \leqslant \text{tr}(x) \leqslant b$: then, the reader can easily verify that

$$\frac{a}{l}\mathbf{e}_l \prec_w x \prec_w b e_1. \tag{2}$$

The following result, that we shall need in the sequel, is a slight strengthening of the previous example.

Lemma 2.2. *Let $\alpha_1, \alpha_2 \in \mathbb{R}^l$ and $\alpha^\downarrow = (\alpha_1, \alpha_2), \beta^\downarrow = (b_1 \mathbf{e}_l, b_2 \mathbf{e}_l) \in \mathbb{R}_{\geqslant 0}^{2l}$ be such that $\text{tr}(\alpha) \geqslant \text{tr}(\beta)$ and $\text{tr}(\alpha_1) \geqslant b_1 l$. Then β is submajorized by α.*

Proof. Since $\text{tr}(\alpha_1) \geqslant b_1 l$ then, by Example 2.1, $b_1 \mathbf{e}_l \prec_w \alpha_1 = (a_1^{(1)}, \ldots, a_l^{(1)})$. Hence, if $1 \leqslant k \leqslant l$ then $\sum_{i=1}^k \alpha_i^\downarrow = \sum_{i=1}^k a_i^{(1)} \geqslant k b_1 = \sum_{i=1}^k \beta_i^\downarrow$. If $\alpha_2 = (a_1^{(2)}, \ldots, a_l^{(2)})$ then define $\gamma = (a_1^{(2)} + (\text{tr}(\alpha_1) - b_1 l), a_2^{(2)}, \ldots, a_l^{(2)})$ and note that $\gamma = \gamma^\downarrow \in \mathbb{R}_{\geqslant 0}^l$. Since $\text{tr}(\gamma) = \text{tr}(\alpha_1) + \text{tr}(\alpha_2) - b_1 l \geqslant b_2 l$ then we conclude again that $b_2 \mathbf{e}_l \prec_w \gamma$. If $1 \leqslant k \leqslant l$ then $\sum_{i=1}^k \gamma_i = \sum_{i=1}^{l+k} \alpha_i^\downarrow - b_1 l \geqslant b_2 k$ and the lemma follows from this last fact. $\square$

(Sub)majorization between vectors is extended by Ando in [1] to (sub)majorization between self-adjoint matrices as follows: given $A, B \in M_l(\mathbb{C})^{sa}$ then we say that A is submajorized by B, and write $A \prec_w B$, if $\lambda(A) \prec_w \lambda(B)$. If we further have that $\text{tr}(A) = \text{tr}(B)$ then we say that A is majorized by B and write $A \prec B$.

Although simple, submajorization plays a central role in optimization problems with respect to convex functionals and unitarily invariant norms, as the following result shows (for a detailed account in majorization and in von Neumann's gauge functions theory see Bhatia's book [5]).

Theorem 2.3. *Let $A, B \in M_l(\mathbb{F})^{sa}$. Then, the following statements are equivalent:*

   (i) $A \prec_w B$.
  (ii) *For every unitarily invariant norm $\| \cdot \|$ in $M_l(\mathbb{F})$ we have $\|A\| \leqslant \|B\|$.*
 (iii) *For every increasing convex function $f : \mathbb{R} \rightarrow \mathbb{R}$ we have $\text{tr}(f(A)) \leqslant \text{tr}(f(B))$.*

Moreover, if $A \prec_w B$ and there exists an increasing strictly convex function $f : \mathbb{R} \to \mathbb{R}$ such that $\mathrm{tr}(f(A)) = \mathrm{tr}(f(B))$ then there exists $U \in \mathcal{U}(l)$ such that $A = U^* B U$.

Recall that given a unitarily invariant norm (henceforth abbreviated u.i.n.) $\| \cdot \|$ in $M_l(\mathbb{C})$ there exists an associated symmetric gauge function $\psi : \mathbb{R}^l \to \mathbb{R}_{\geqslant 0}$ such that $\|A\| = \psi(s(A))$, where $s(A) = \lambda(|A|) \in \mathbb{R}^l$ is the vector of singular values of A. Next we describe a particular class of u.i.n.'s that we shall consider in the sequel.

Definition 2.4. A sequence $\{\| \cdot \|_n\}_n$ such that for each $n \in \mathbb{N}$ $\| \cdot \|_n$ is a u.i.n. in $M_n(\mathbb{F})$ is compatible if, for every $X \in M_r(\mathbb{F})$ then

$$\left\| \begin{pmatrix} X & 0 \\ 0 & \mathbf{0}_t \end{pmatrix} \right\|_{r+t} = \|X\|_r, \tag{3}$$

where $\mathbf{0}_t \in M_t(\mathbb{R})$ is the zero matrix. If ψ_n is the symmetric gauge function associated with $\| \cdot \|_n$ then, (3) is equivalent to $\psi_{r+t}(x, 0_t) = \psi_r(x)$, where $x \in \mathbb{R}^r$ and $0_t \in \mathbb{R}^t$ is the zero vector. In this case, we simply write $\| \cdot \|$ and ψ respectively to denote the norms and functions of any order.

Let $V : \mathcal{H} \to \mathcal{K}$ be a linear operator and assume that $\dim \mathcal{H} = d > l = \dim \mathcal{K}$. Then, it is well known that there exists a unitary operator $U \in \mathcal{U}(d)$ such that

$$U^* \begin{pmatrix} VV^* & 0 \\ 0 & \mathbf{0}_{d-l} \end{pmatrix} U = V^* V,$$

where the above block matrix representation is with respect to the decomposition $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}'$ as described in the preliminaries. Hence, if $\| \cdot \|$ is a compatible u.i.n. in the sense of Definition 2.4 it holds that $\|VV^*\| = \|V^*V\|$. This last equality is our main motivation to consider these norms.

We shall use systematically the following facts, that are an elementary consequence of the previous results: if $\| \cdot \|$ is an arbitrary u.i.n. in $M_l(\mathbb{F})$ with associated symmetric gauge function ψ then, for every $A \in M_l(\mathbb{F})^+$ (resp. $x \in \mathbb{R}^l_{\geqslant 0}$) we have

$$\|A\| \geqslant \frac{\mathrm{tr}(A)}{l} \|I_l\| = \mathrm{tr}(A)\eta_\psi(l) \quad (\text{resp. } \psi(x) \geqslant \frac{\mathrm{tr}(x)}{l} \psi(\mathbf{e}_l) = \mathrm{tr}(x)\eta_\psi(l)),$$

where $\eta_\psi(l) = \frac{\|I_l\|}{l} = \frac{\psi(\mathbf{e}_l)}{l}$, since $\frac{\mathrm{tr}(A)}{l} \mathbf{e}_l \prec \lambda(A)$ and $\frac{\mathrm{tr}(x)}{l} \mathbf{e}_l \prec x$ respectively.

Definition 2.5. A compatible u.i.n. $\| \cdot \|$ is strict if, for any $A \in M_l(\mathbb{F})^+$ then

$$\|A\| = \mathrm{tr}(A)\eta_\psi(l) \Rightarrow A = \frac{\mathrm{tr}(A)}{l} I,$$

where ψ is the symmetric gauge function associated with $\| \cdot \|$ and $\eta_\psi(l) = \frac{\psi(\mathbf{e}_l)}{l}$. Equivalently, $\| \cdot \|$ is strict if for $x \in \mathbb{R}^l_{\geqslant 0}$ such that $\psi(x) = \mathrm{tr}(x)\eta_\psi(l)$ then $x = \frac{\mathrm{tr}(x)}{l} \mathbf{e}_l$.

Examples 2.6. As an example of compatible unitarily invariant norm, let us consider the p-norms $\| \cdot \|_p$, with $1 \leqslant p \leqslant \infty$. On the other hand, if $1 < p \leqslant \infty$ then $\| \cdot \|_p$ is an strict norm. Moreover, if $1 < p < \infty$ then $f_p(x) = x^p$ is an strictly convex function and hence the following stronger property holds (see Theorem 2.3): if $A, B \in M_l(\mathbb{C})^{sa}$ are such that $A \prec_w B$ and $\|A\|_p = \|B\|_p$ then, $A = U^* B U$ for some $U \in \mathcal{U}(l)$.

2.2. Klyachko's and Fulton's spectral theory on sums of hermitian matrices

In what follows we describe the basic facts about the spectral characterization of the sums of hermitian matrices obtained by Klyachko [24] and Fulton [18], related with A. Horn's saturation conjecture solved by Knutson and Tao [25].

Let $\mathcal{S}_r^d = \{(j_1,\ldots,j_r) : 1 \leqslant j_1 < j_2 \cdots < j_r \leqslant d\}$. For $J = (j_1,\ldots,j_r) \in \mathcal{S}_r^d$, define the associated partition

$$\lambda(J) = (j_r - r,\ldots,j_1 - 1).$$

Denote by $LR_r^d(m)$ the set of $(m+1)$-tuples $(J_0,\ldots,J_m) \in (\mathcal{S}_r^d)^{(m+1)}$, such that the Littlewood–Richardson coefficient of the associated partitions $\lambda(J_0),\ldots,\lambda(J_m)$ is positive, i.e., one can generate the Young diagram of $\lambda(J_0)$ from those of $\lambda(J_1),\ldots,\lambda(J_m)$ according to the Littlewood–Richardson rule (see [17]). With these notations and terminologies we have

Theorem 2.7. Let $\lambda_i = \lambda_i^{\downarrow} = (\lambda_1^{(i)},\ldots,\lambda_d^{(i)}) \in \mathbb{R}^d$ for $i = 0,\ldots,m$. Then, the following statements are equivalent:

(i) There exists $A_i \in M_d(\mathbb{C})^{sa}$ with $\lambda(A_i) = \lambda_i$ for $0 \leqslant i \leqslant m$ and such that

$$A_0 = A_1 + \cdots + A_m.$$

(ii) For each $r \in \{1,\ldots,d\}$ and $(J_0,\ldots,J_m) \in LR_r^d(m)$ we have

$$\sum_{j \in J_0} \lambda_j^{(0)} \leqslant \sum_{i=1}^{m} \sum_{j \in J_i} \lambda_j^{(i)} \tag{4}$$

plus the condition $\sum_{j=1}^{d} \lambda_j^{(0)} = \sum_{i=1}^{m} \sum_{j=1}^{d} \lambda_j^{(i)}$.

We shall refer to the inequalities in (4) as *Horn–Klyachko's compatibility inequalities*.
For comments on further developments related with the previous theorem see Remark 5.2

3. Optimality of (m, l, d)-protocols for the q-potential

In what follows we consider (m, l, d)-reconstruction systems, which are more general system of operators than those considered in [4,6,7,8,19,29], that also have an associated reconstruction algorithm. In what follows $\mathcal{H}$ and $\mathcal{K}$ denote (real or complex) Hilbert spaces of dimensions d and l respectively, with $l < d$.

Definition 3.1. A family $\{V_i\}_{i=1}^{m}$ is an (m, l, d)-reconstruction system if for $1 \leqslant i \leqslant m$, $V_i : \mathcal{H} \to \mathcal{K}$ are linear transformations such that $\sum_{i=1}^{m} V_i^* V_i = S$ is an invertible (positive) operator.

Notice that an $(m, 1, d)$-reconstruction system is a frame [9] in the usual sense.
Recall that an (m, l, d)-protocol on the Hilbert space $\mathcal{H}$ [6] is a family $\{V_i\}_{i=1}^{m}$ such that $V_i : \mathcal{H} \to \mathcal{K}$ for $1 \leqslant i \leqslant m$ and $\sum_{i=1}^{m} V_i^* V_i = I_d$ (see also [7], where protocols are related to C^*-encodings with noiseless subsystems). Clearly, (m, l, d)-protocols are (m, l, d)-reconstruction systems in the sense of Definition 3.1.
If $\{V_i\}_{i=1}^{m}$ is an (m, l, d)-reconstruction system then we consider its *analysis operator* $V : \mathcal{H} \to \oplus_{i=1}^{m}\mathcal{K}$ given by $Vx = \oplus_{i=1}^{m} V_i x$; similarly, we consider its *synthesis operators* given by V^*, i.e., $V^* \oplus_{i=1}^{m} y_i = \sum_{i=1}^{m} V_i^* y_i$. For a general (m, l, d)-reconstruction system $\{V_i\}_i$ such that $\sum_{i=1}^{m} V_i^* V_i = S$ we have

$$\sum_{i=1}^{m} S^{-1} V_i^* V_i = I_d \quad \text{and} \quad \sum_{i=1}^{m} V_i^* V_i S^{-1} = I_d$$

and thus, we obtain the reconstruction formulas

$$x = \sum_{i=1}^{m} S^{-1} V_i^* (V_i x) = \sum_{i=1}^{m} V_i^* V_i (S^{-1} x).$$

In this context S is called the *reconstruction system operator* of $\{V_i\}_i$ while $G = VV^*$ is called the *Grammian operator* of $\{V_i\}_i$. It is easy to see that in this case $\{V_i S^{-1}\}_{i=1}^{m}$ is also an (m, l, d)-reconstruction

system, that we call the *dual* reconstruction system associated to $\{V_i\}_i$; indeed the reconstruction system operator of the this dual is S^{-1}.

For practical purposes, an encoding–decoding scheme based on the (m, l, d)-reconstruction system above involves the problem of inverting the reconstruction system operator S. One of the advantages of considering (m, l, d)-protocols for applications is that the reconstruction system operator in this case is I_d. As we shall see (m, l, d)-protocols are optimal in other senses, too.

In the seminal work [4] Benedetto and Fickus introduced the so-called frame potential, as a potential function for the frame force. The structure of minimizers of the frame potential under several restrictions [4,10,11,29] have been obtained, since these are considered as stable configurations with respect to the frame force. This has motivated possible physical interpretations of families of frames, such as (uniform) tight frames [11]. Moreover, in [29] it is shown that the minimizers of the frame potential (under suitable restrictions) have structural properties implying their stability with respect to a more general family of convex functionals that contains the frame potential of Benedetto and Fickus.

In what follows we introduce the q-potential of a reconstruction system (regardless of an underlying force inducing this potential), which is a positive semi-definite matrix. Then, we consider two optimization problems associated with this potential (see Theorems 3.3 and 3.4 below).

Definition 3.2. Let $\{V_i\}_{i=1}^m$ be an (m, l, d)-reconstruction system on the Hilbert space $\mathcal{H}$. Then, the q-potential of the reconstruction system is defined as

$$\mathbf{P}_q(V) = \sum_{i,j=1}^m |V_i V_j^*|^2 \in M_l(\mathbb{C})^+.$$

It is straightforward that the q-potential above is the value $\mathrm{Tr}_m((VV^*)^2) \in M_l(\mathbb{C})$, i.e., the partial trace of the square of the Grammian operator VV^* with respect to the block representation $M_{m \cdot l}(\mathbb{F}) = M_m(M_l(\mathbb{F}))$. Note that the q-potential coincides with the Benedetto–Fickus potential in the case $l = 1$. In contrast to the Benedetto–Fickus potential, there is no natural way a priori to compare the q-potential of two (m, l, d)-reconstruction systems when $l > 1$.

In order to state the following result we recall some distinguished classes of protocols. We say that an (m, l, d)-protocol $\{V_i\}_i$ is *projective* if for each $1 \leqslant i \leqslant m$ then $V_i^* V_i = w_i P_i$, where P_i is an orthogonal projection in $M_d(\mathbb{C})$ and $w_i > 0$ are called the associated weights. If the weights of a projective (m, l, d)-protocol are equal then we say that it is uniformly weighted (and we abbreviate this by u.w.p). Finally, we say that an (m, l, d)-protocol is *rank-l*, if $\mathrm{rank}(V_i^*) = l$ for $1 \leqslant i \leqslant m$. Notice that if $\{V_i\}_i$ is a rank-l projective (m, l, d)-protocol then $V_i V_i^* = w_i I_l$ with $w_i > 0$, for $1 \leqslant i \leqslant m$.

Theorem 3.3 (Optimality of general protocols). *Let* $\{V_i\}_{i=1}^m$ *be an* (m, l, d)-*reconstruction system on the Hilbert space* $\mathcal{H}$ *such that* $\mathrm{tr}(V^*V) = \sum_{i=1}^m \mathrm{tr}(V_i^*V_i) \geqslant d$. *Then,*

$$\frac{d}{l} I_l \prec_w \mathbf{P}_q(V). \tag{5}$$

Hence, for every u.i.n. $\| \cdot \|$ *on* $M_l(\mathbb{C})$ *with associated symmetric gauge function* ψ *we have*

$$d \cdot \eta_\psi(l) \leqslant \|\mathbf{P}_q(V)\| \tag{6}$$

and for every increasing convex function $f : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ *with* $f(0) = 0$ *we have*

$$l \cdot f\left(\frac{d}{l}\right) \leqslant \mathrm{tr}(f(\mathbf{P}_q(V))). \tag{7}$$

If majorization holds in (5) *or there exists u.i.n.* $\| \cdot \|$ *such that equality holds in* (6) *or if there exists an increasing strictly convex function* $f : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ *with* $f(0) = 0$ *such that equality holds in* (7) *then* $\{V_i\}$ *is an* (m, l, d)-*protocol.*

Conversely, if $\{V_i\}_i$ *is a projective rank-l* (m, l, d)-*protocol then majorization holds in* (5) *and the lower bounds in* (6) *and* (7) *are attained for each u.i.n. and each function as above, respectively.*

Proof. Since $\mathrm{tr}(V^*V) \geq d$ then it follows that $I_d \prec_w V^*V \in M_d(\mathbb{C})$ and thus $d = \mathrm{tr}(I_d^2) \leq \mathrm{tr}((V^*V)^2) = \mathrm{tr}((VV^*)^2)$. Hence,

$$d \leq \mathrm{tr}((VV^*)^2) = \mathrm{tr}(\mathbf{P}_q(V)) \quad \Rightarrow \quad \frac{d}{l}I_l \prec_w \mathbf{P}_q(V) \in M_l(\mathbb{C}). \tag{8}$$

Notice that (6) and (7) are consequences of this last fact (see the comments after Example 2.6).

Assume that majorization holds in (5), so then we have

$$\mathrm{tr}(I_d^2) = \mathrm{tr}\left(\frac{d}{l}I_l\right) = \mathrm{tr}(\mathbf{P}_q(V)) = \mathrm{tr}((VV^*)^2) = \mathrm{tr}((V^*V)^2).$$

Since $I_d \prec_w V^*V$ and the function $f(x) = x^2$ is strictly convex, by Theorem 2.3 we conclude that there exists a unitary $U \in \mathcal{U}(d)$ such that

$$V^*V = U^*(I_d)U = I_d.$$

If there exists an u.i.n. $\|\cdot\|$ such that equality holds in (6) then, using the left-hand side of (8) we get

$$d \cdot \eta_\psi(l) = \|\mathbf{P}_q(V)\| \geq \mathrm{tr}(\mathbf{P}_q(V)) \cdot \eta_\psi(l) \geq d \cdot \eta_\psi(l), \tag{9}$$

which implies that $\mathrm{tr}((V^*V)^2) = \mathrm{tr}(\mathbf{P}_q(V)) = d$. As before, we conclude that $V^*V = I_d$. On the other hand, if there exists an increasing strictly convex function f for which equality holds in (7) then, since $\frac{d}{l}I_l \prec_w \mathbf{P}_q(V)$, we conclude from Theorem 2.3 that $\mathrm{tr}(\mathbf{P}_q(V)) = d$ and hence that $V^*V = I_d$.

Finally, it is clear that in case $\{V_i\}_i$ is a projective rank-l (m, l, d)-protocol then $\mathbf{P}_q(V) = \frac{d}{l}I_l$. The last part of the theorem follows from this fact. $\quad\square$

Theorem 3.4 (Optimality of u.w.p. protocols). *Let $\{V_i\}_{i=1}^m$ be an (m, l, d)-reconstruction system on the Hilbert space $\mathcal{H}$ such that $\mathrm{tr}((V_i^*V_i)^{1/2}) \geq \left(\frac{d \cdot l}{m}\right)^{1/2}$ for $1 \leq i \leq m$. Then,*

$$\frac{d}{l}I_l \prec_w \mathbf{P}_q(V). \tag{10}$$

Hence, for every u.i.n. $\|\cdot\|$ on $M_l(\mathbb{C})$ with associated symmetric gauge function ψ we have

$$d \cdot \eta_\psi(l) \leq \|\mathbf{P}_q(V)\| \tag{11}$$

and for every increasing convex function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(0) = 0$ we have

$$l \cdot f(\frac{d}{l}) \leq \mathrm{tr}(f(\mathbf{P}_q(V))). \tag{12}$$

Moreover, majorization holds in (10) or there exists u.i.n. $\|\cdot\|$ such that equality holds in (11) or there exists an increasing strictly convex function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(0) = 0$ such that equality holds in (12) if and only if $\{V_i\}_i$ is a u.w.p. rank-l (m, l, d)-protocol.

Proof. Let $\{V_i\}_i$ be an (m, l, d)-reconstruction system such that, for $1 \leq i \leq m$

$$\mathrm{tr}((V_i^*V_i)^{1/2}) = \mathrm{tr}((V_iV_i^*)^{1/2}) = \left(\frac{d \cdot l}{m}\right)^{1/2} \quad \Rightarrow \quad \left(\frac{d}{ml}\right)^{1/2}I_l \prec_w (V_iV_i^*)^{1/2}$$

and thus $\mathrm{tr}(V_i^*V_i) = \mathrm{tr}(V_iV_i^*) \geq \mathrm{tr}\left(\frac{d}{ml}I_l\right) = \frac{d}{m}$. Hence, $\sum_{i=1}^m \mathrm{tr}(V_i^*V_i) \geq d$ and thus (10), (11) and (12) are consequences of Theorem 3.3. If majorization holds in (10) or there exists u.i.n. $\|\cdot\|$ such that equality holds in (11) or there exists an increasing strictly convex function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $f(0) = 0$ such that equality holds in (12) then, again by Theorem 3.3, we conclude that $\{V_i\}$ is an (m, l, d)-protocol. Thus, $\mathbf{P}_q(V) = \sum_{i=1}^m V_iV_i^*$ with $\mathrm{tr}(\mathbf{P}_q(V)) = d$. Therefore, $\mathrm{tr}(V_iV_i^*) = \frac{d}{m}$ and since $\left(\frac{d}{ml}\right)^{1/2}I_l \prec_w (V_iV_i^*)^{1/2}$ (recall that $f(x) = x^2$ is an strictly convex function) we conclude as before that $V_i^*V_i = \frac{d}{ml}P_i$ for some rank-l orthogonal projection P_i for $1 \leq i \leq m$. $\quad\square$

There are other issues regarding this potential, such as the structure of local minimizers where we consider the relativization of the product topology in $\prod_{i=1}^{m} \mathcal{L}(\mathcal{H}, \mathcal{K})$, to the sets of reconstruction systems considered in the previous theorems. This topic has recently been considered in [30].

Remark 3.5. There are other criteria with respect to which (u.w.p.) (m, l, d)-protocols are optimal in the class of (m, l, d)-reconstruction systems satisfying some further restrictions. For example, consider the class $\mathcal{R}(m, l, d)$ of all (m, l, d)-reconstruction systems $\{V_i\}_{i=1}^{m}$ for which its associated reconstruction system operator S is a contraction, i.e., $\|S\|_{\infty} \leqslant 1$, where $\| \cdot \|_{\infty}$ denotes the spectral (operator) norm. A natural measure of stability for an (m, l, d)-reconstruction system $\{V_i\}_i \in \mathcal{R}(m, l, d)$ is $\|S^{-1}\|$, where S is the reconstruction system operator of $\{V_i\}_i$ and $\| \cdot \|$ denotes a fixed u.i.n. in $M_d(\mathbb{F})$; we are then interested in minimizing $\|S^{-1}\|$. Equivalently, we are interested in minimizing the norm of (the reconstruction system operator of) the dual reconstruction system.

Notice that if $\lambda(S^{-1}) \in \mathbb{R}^d$ denotes the vector of eigenvalues of S^{-1} then $\lambda_i(S^{-1}) \geqslant 1$ for $1 \leqslant i \leqslant d$, so that $\operatorname{tr}(S^{-1}) \geqslant d$. Therefore (see the comments before Definition 2.5) $I_d \prec_w S^{-1}$. Hence, Theorem 2.3 implies that

$$\|S^{-1}\| \geqslant \|I_d\|. \tag{13}$$

Notice that this lower bound is attained whenever $\{V_i\}$ is an (m, l, d)-protocol.

Moreover, if we further assume that $\| \cdot \|$ is a strict u.i.n. (e.g. the Frobenius or the operator norm) then the inequality (13) is attained for $\{V_i\}_i \in \mathcal{R}(m, l, d)$ if and only if $\{V_i\}_i$ is an (m, l, d)-protocol, i.e., if and only if $S = I_d$. Indeed, if $\|S^{-1}\| = \|I_d\|$ then the inequalities $\|S^{-1}\| \geqslant \operatorname{tr}(S^{-1}) \cdot \eta_\psi(d) \geqslant \|I_d\|$ imply that $\|S^{-1}\| = \operatorname{tr}(S^{-1}) \cdot \eta_\psi(d)$, where ψ is the gauge function associated with $\| \cdot \|$. Thus $S^{-1} = I_d$ since $\| \cdot \|$ is strict.

We can similarly introduce restrictions to each coordinate operator of an (m, l, d)-reconstruction system in order that u.w.p. (m, l, d)-protocols are the minimizers of $\|S^{-1}\|$ for an strict u.i.n. $\| \cdot \|$. These facts strengthen the idea developed in Theorems 3.3 and 3.4 that protocols play an special (important) role within the class of general reconstruction systems.

4. Optimal protocols for erasures and strict compatible u.i.n.

Following [6] (see also [8,19]) we begin by modeling the situation in which in an encoding–decoding scheme based on an (m, l, d)-protocol some fixed number of packets ($V_i x$) are lost, corrupted or just delayed for such a long time that we decide to reconstruct x without these packets.

In order to model the previous situation we consider a signal as a vector in the d-dimensional (real or complex) vector space $\mathcal{H}$, which is transmitted in the form of m packets of l coefficients. Hence, each packet is a vector the l-dimensional (real or complex) Hilbert space $\mathcal{K}$. We shall assume that $d < ml$ to allow for redundancy of the information sent through the channel and thus for the possibility of a reasonable reconstruction even when some packets are lost in the transmission. On the other hand, we shall also assume that $l < d$, i.e., the dimension (complexity) of the data is strictly bigger that the dimension of the noiseless sub-channel (subsystem) which constitute the packets (otherwise there are trivial optimal schemes).

Given $\mathbb{K} \subseteq \mathbb{J} := \{1, \ldots, m\}$ a subset of size $|\mathbb{K}| = p$ we consider the associated *packet-lost operator* $E_{\mathbb{K}}$ on $\bigoplus_{j=1}^{m} \mathcal{K}$ given by $E_{\mathbb{K}}(\bigoplus_{j=1}^{m} y_j) = \bigoplus_{j=1}^{m} (1 - \chi_{\mathbb{K}}(i)) y_i$, where $\chi_{\mathbb{K}} : \mathbb{J} \to \{0, 1\}$ denotes the characteristic function of the set $\mathbb{K} \subset \mathbb{J}$. We denote $D_{\mathbb{K}} := I - E_{\mathbb{K}}$. In order to simplify the notation we write E_j (respectively D_j) in case $\mathbb{K} = \{j\}$.

In our present situation, we shall consider a "blind reconstruction" strategy for (m, l, d)-protocols for $\mathcal{H}$. In case some packets are lost, i.e., assuming that the encoded information $Vx \in \bigoplus_{i=1}^{m} \mathcal{K}$ (for some $x \in \mathcal{H}$) is altered according to the packet-lost operator $E_{\mathbb{K}}$, our reconstructed vector will be $V^* E_{\mathbb{K}} V(x)$, where V denotes the analysis operator of the (m, l, d)-protocol $\{V_i\}_{i=1}^{m}$.

As a measure of performance of an (m, l, d)-protocol in this setting we introduce the worst case reconstruction error when p packets are lost with respect to an arbitrary compatible unitarily invariant norm:

$$e_p^\psi (V) := \max\{\|V^*V - V^*E_\mathbb{K}V\| \, : \, \mathbb{K} \subseteq \mathbb{J}, \, |\mathbb{K}| = p\},$$

where $\| \cdot \|$ is a compatible u.i.n. with associated symmetric gauge function ψ (see Definition 2.4) and V denotes the analysis operator of the (m, l, d)-protocol $\{V_i\}_{i=1}^m$. Since the set $\mathcal{V}(m, l, d)$ of all (m, l, d)-protocols is compact then the value

$$e_1^\psi (m, l, d) = \inf\{e_1^\psi (V) \, : \, \{V_i\}_i \in \mathcal{V}(m, l, d)\}$$

is attained and we define the set of *1-loss optimal protocols for* $\| \cdot \|$ to be the non-empty compact set $\mathcal{V}_1^\psi (m, l, d)$ where this infimum is attained, i.e.,

$$\mathcal{V}_1^\psi (m, l, d) := \{\{V_i\}_i \in \mathcal{V}(m, l, d) : e_1^\psi (V) = e_1^\psi (m, l, d)\}.$$

Proceeding inductively, we now set for $1 \leqslant p \leqslant m$

$$e_p^\psi (m, l, d) = \inf\{e_p^\psi (V) \, : \, \{V_i\}_i \in \mathcal{V}_{p-1}^\psi(m, l, d)\}$$

and define $\mathcal{V}_p^\psi (m, l, d)$, the *optimal p-protocols for* $\| \cdot \|$, to be the non-empty compact subset of $\mathcal{V}_{p-1}^\psi$ (m, l, d) where this infimum is attained.

4.1. $e_1^\psi (\cdot)$ optimality for one package lost

Lemma 4.1. *Let* $\| \cdot \|$ *be a compatible u.i.n. with associated symmetric gauge function* ψ. *Let* $\{V_i\}_{i=1}^m$ *be an* (m, l, d)-*protocol on the Hilbert space* $\mathcal{H}$. *Then,*

$$\max_{1 \leqslant j \leqslant m} \|V_j V_j^*\| \geqslant \frac{d \cdot \eta_\psi (l)}{m}. \tag{14}$$

where $\eta_\psi (l) = \frac{\psi(\mathbf{e}_l)}{l}$. *Moreover, if* $\| \cdot \|$ *is strict then equality holds in* (14) *if and only if* $\{V_i\}_{i=1}^m$ *is a u.w.p. rank-l* (m, l, d)-*protocol.*

Proof. Following [6] we consider

$$\max_j \|V_j V_j^*\| \geqslant \frac{1}{m} \sum_{j=1}^m \|V_j V_j^*\|. \tag{15}$$

Recall that in this case $\frac{\mathrm{tr}(V_j V_j^*)}{l} \, \mathbf{e}_l \prec \lambda(V_j V_j^*)$ and hence

$$\|V_j V_j^*\| \geqslant \frac{\mathrm{tr}(V_j V_j^*)}{l} \, \psi(\mathbf{e}_l) = \mathrm{tr}(V_j V_j^*)\eta_\psi (l). \tag{16}$$

Using the fact that $\sum_{i=1}^m \mathrm{tr}(V_j V_j^*) = d$, (14) now follows from (15) and (16).

Assume further that $\| \cdot \|$ is strict and the equality holds in (14). Then, equality also hold in (15) and (16), too. Since $\| \cdot \|$ is strict we conclude that $\lambda(V_j V_j^*) = \frac{\mathrm{tr}(V_j V_j^*)}{l}\mathbf{e}_l$ and hence $V_j^* V_j$ is a multiple (independent of j) of a rank-l projection. The lemma easily follows from these facts. $\square$

Theorem 4.2. *Let* $\| \cdot \|$ *be a compatible u.i.n. with associated symmetric gauge function* ψ. *Let* $\{V_i\}_{i=1}^m$ *be the coordinate operators of an* (m, l, d)-*protocol on the Hilbert space* $\mathcal{H}$. *Then,*

$$e_1^\psi (V) \geqslant \frac{d \cdot \eta_\psi (l)}{m}. \tag{17}$$

Moreover, if $\| \cdot \|$ *is strict then equality holds in* (17) *if and only if* $\{V_i\}_{i=1}^m$ *is a u.w.p. rank-l* (m, l, d)-*protocol.*

Proof. For fixed $1 \leqslant j \leqslant m$ note that $V^*V - V^*E_j V = V^*D_j V$ and

$$\|V^*D_j V\| = \|D_j VV^* D_j\| = \|V_j V_j^*\| = \|V_j^* V_j\|.$$

Therefore, the quantity to be minimized is $e_1^\psi(V) = \max_j \|V_j^* V_j\|$. The result now follows from the previous lemma. □

The previous theorem completely characterizes the structure of the 1-loss optimal (m, l, d)-protocols in case $\|\cdot\|$ is an strict compatible u.i.n. Since the operator norm is a compatible strict u.i.n. we derive in particular [6, Theorem 13] (note that for the operator norm $\|\cdot\|_\infty$ we have $\eta_\infty(l) = \frac{1}{l}$). In Section 5 we shall be concerned with the existence of protocols with prescribed properties (such as u.w.p. rank-l (m, l, d)-protocols).

4.2. The case of two lost packages

Consider the quantity defined in [6]

$$c_{m,l,d} := \sqrt{\frac{d}{(m-1)\,ml}\left(1 - \frac{d}{ml}\right)}.$$

In what follows we consider the class

$$\mathcal{C}(m, l, d) = \{\{V_i\}_i : \text{ u.w.p. rank} - l\ (m, l, d)\text{protocol}, \max_{1 \leqslant i \neq j \leqslant m} \text{tr}(|V_i V_j^*|) \geqslant l \cdot c_{m,l,d}\}.$$

Theorem 4.3 (e_2^ψ optimality in $\mathcal{C}(m, l, d)$). *Let $\|\cdot\|$ be a compatible u.i.n. with associated symmetric gauge function ψ. Then, if $\{V_i\}_i \in \mathcal{C}(m, l, d)$ we have that*

$$e_2^\psi(V) \geqslant \psi\left(\left(\frac{d}{ml} + c_{m,l,d}\right)\mathbf{e}_l, \left(\frac{d}{ml} - c_{m,l,d}\right)\mathbf{e}_l\right). \tag{18}$$

If $\{V_i\}_i$ is a u.w.p rank-l (m, l, d) protocol such that for $i \neq j\,V_i V_j^* = c_{m,l,d}Q_{ij}$ for unitary operators on $\mathcal{K}$, then $\{V_i\}_i \in \mathcal{C}(m, l, d)$ and it attains the bound for e_2^ψ in (18).

Proof. In order to compute the worst case reconstruction error for two lost packages we note that if $\|\cdot\|$ is a compatible u.i.n. then (see the comments after Definition 2.4 in Section 2)

$$\|V^*(D_i + D_j)V\| = \|(D_i + D_j)VV^*(D_i + D_j)\| = \left\|\begin{pmatrix} \frac{d}{ml}I & V_i V_j^* \\ V_j V_i^* & \frac{d}{ml}I \end{pmatrix}\right\|$$

$$= \psi\left(\left(\frac{d}{ml}\mathbf{e}_l + s(V_i V_j^*), \frac{d}{ml}\mathbf{e}_l - s(V_i V_j^*)\right)\right).$$

where the last equality above follows from [20, Theorem 7.3.7] and $s(A) = \lambda(|A|) \in \mathbb{R}^l$ is the vector of singular values of $A \in M_l(\mathbb{C})$. Notice that for $i \neq j$

$$\text{tr}\left(\left(\frac{d}{ml}\mathbf{e}_l + s(V_i V_j^*), \frac{d}{ml}\mathbf{e}_l - s(V_i V_j^*)\right)\right) = 2\frac{d}{m} \tag{19}$$

and since $\{V_i\}_i \in \mathcal{C}(m, l, d)$ then, for some fixed $i_0 \neq j_0$ we should have

$$\text{tr}\left(\left(\frac{d}{ml}\mathbf{e}_l + s(V_{i_0} V_{j_0}^*)\right)\right) = \frac{d}{m} + \text{tr}(|V_{i_0} V_{j_0}^*|) \geqslant \frac{d}{m} + l \cdot c_{m,l,d}. \tag{20}$$

Now, (19), (20) and Lemma 2.2 imply that in this case

$$\left(\left(\frac{d}{ml} + c_{m,l,d}\right)\mathbf{e}_l, \left(\frac{d}{ml} - c_{m,l,d}\right)\mathbf{e}_l\right) \prec \left(\frac{d}{ml}\mathbf{e}_l + s(V_{i_0} V_{j_0}^*), \frac{d}{ml}\mathbf{e}_l - s(V_{i_0} V_{j_0}^*)\right).$$

Therefore,

$$e_2^\psi(V) \geqslant \|V^*(D_{i_0} + D_{j_0})V\| \geqslant \psi\left(\left(\frac{d}{ml} + c_{m,l,d}\right)\mathbf{e}_l, \left(\frac{d}{ml} - c_{m,l,d}\right)\mathbf{e}_l\right).$$

Finally, is clear that in case that $\{V_i\}_i$ is such that for $i \neq j$, $V_i V_j^* = c_{m,l,d} Q_{i,j}$ for unitary operators on $\mathcal{K}$, then $\{V_i\}_i \in \mathcal{C}(m, l, d)$ and it attains the bound of e_2^{ψ} in (18). $\square$

It would be interesting to characterize the structure of all u.w.p. rank-l (m, l, d)-protocols that attain the lower bound in (18) in the general context of compatible u.i.n. On the other hand, it is not clear at this point whether the condition in the definition of the class $\mathcal{C}(m, l, d)$ is not trivial, i.e., it holds for every u.w.p. protocol (see also Lemma 4.4 and Theorem 4.6).

The following facts are known for $l = 1$ (see [19]).

Lemma 4.4. Let $\| \cdot \|$ be a compatible u.i.n. with associated symmetric gauge function ψ. Let $\{V_i\}_{i=1}^m$ be a u.w.p. rank-l (m, l, d)-protocol on the Hilbert space $\mathcal{H}$. Then, for every $1 \leqslant i \leqslant m$ we have

$$\sum_{j=1, j \neq i}^m \mathrm{tr}(|V_j V_i^*|^2) = \frac{d}{m}\left(1 - \frac{d}{ml}\right), \tag{21}$$

$$\sum_{j=1, j \neq i}^m \mathrm{tr}(|V_i V_j^*|) \geqslant \sqrt{\frac{d}{ml}\left(1 - \frac{d}{ml}\right)} \cdot l \tag{22}$$

and hence

$$\max_{1 \leqslant j \leqslant m, \, i \neq j} \mathrm{tr}(|V_i V_j^*|^2) \geqslant c_{m,l,d}^2 \cdot l, \tag{23}$$

$$\max_{1 \leqslant j \leqslant m, \, i \neq j} \mathrm{tr}(|V_i V_j^*|) \geqslant \max\left(\frac{c_{m,l,d} \cdot l}{\sqrt{m-1}}, c_{m,l,d} \cdot \sqrt{l}\right). \tag{24}$$

Proof. Since $VV^* = (VV^*)^2$ then, for fixed $1 \leqslant i \leqslant m$

$$\frac{d}{ml} I_l = V_i V_i^* = \sum_{j=1}^m |V_j V_i^*|^2 = \sum_{j=1, j \neq i}^m |V_j V_i^*|^2 + \frac{d^2}{m^2 l^2} I_l. \tag{25}$$

Now (21) follows by taking traces in (25). Using again (25) and the concavity of the square root function [31] we get

$$\sum_{j=1, j \neq i}^m \mathrm{tr}(|V_j V_i^*|) \geqslant \mathrm{tr}\left(\sqrt{\left(\frac{d}{ml} - \frac{d^2}{m^2 l^2}\right) I_l}\right)$$

which is (22). Now, from (21) we get (23). Using (23) we get that, for fixed $1 \leqslant i \leqslant m$

$$\max_{1 \leqslant j \leqslant m, \, i \neq j} \mathrm{tr}(|V_i V_j^*|) \geqslant \max_{1 \leqslant j \leqslant m, \, i \neq j} \mathrm{tr}(|V_i V_j^*|^2)^{1/2} \geqslant \sqrt{c_{m,l,d}^2 \cdot l}. \tag{26}$$

Finally, from (22) and using (26) we get (24). $\square$

Remark 4.5. Under the hypothesis of Lemma 4.4, note that (23) implies that, for fixed $1 \leqslant i \leqslant m$ then

$$\max_{1 \leqslant j \leqslant m, i \neq j} \||V_i V_j^*|^2\| \geqslant \frac{1}{m-1} \sum_{1 \leqslant j \leqslant m, i \neq j} \||V_i V_j^*|^2\| \geqslant$$

$$c_{m,l,d}^2(\psi) := \frac{1}{m-1} \sum_{1 \leqslant j \leqslant m, i \neq j} \mathrm{tr}(|V_i V_j^*|^2) \eta_\psi(l) = \frac{d \cdot \eta_\psi(l)}{m(m-1)}\left(1 - \frac{d}{ml}\right).$$

If we assume further that $\| \cdot \|$ is strict and that for fixed $1 \leqslant i \leqslant m$

$$\max_{1 \leqslant j \leqslant m, i \neq j} \||V_i V_j^*|^2\| = c_{m,l,d}^2(\psi)$$

then, for every $j \neq i$, $|V_i V_j^*|$ has only one eigenvalue, namely $c_{m,l,d}$. Using the polar decomposition for $V_i V_j^*$ we conclude that $V_i V_j^* = c_{m,l,d} Q_{i,j}$ for some unitary operator $Q_{i,j}$ in $\mathcal{K}$. In particular,

$$\max_{1 \leq i \neq j \leq m} \||V_i V_j^*|^2\| \geq c_{m,l,d}^2(\psi) \tag{27}$$

and equality holds if and only if, for $1 \leq i \neq j \leq m$ then $V_i V_j^* = c_{m,l,d} Q_{ij}$ for unitary operators Q_{ij} in $\mathcal{K}$. These remarks generalize to this context [6, Lemma 14] for the spectral norm (notice that in this case $\eta_\infty(l) = \frac{1}{l}$); in particular, (27) is an extension of a result of Welch [34].

Given a compatible strict u.i.n. $\| \cdot \|$ we say that it is k-strongly strict if for every $A, B \in M_k(\mathbb{C})^{sa}$ such that $A \prec B$ and $\|A\| = \|B\|$ then $A = U^* B U$ for some $U \in \mathcal{U}(k)$. For example, the p-norms are k-strongly strict for $k \geq 1$ (see Example 2.6). On the other hand, it is easy to see that the operator norm is 2-strongly strict.

Theorem 4.6. *Let $\| \cdot \|$ be a compatible u.i.n. with associated symmetric gauge function ψ.*

(i) *If $\{V_i\}_i$ is a u.w.p. $(m, 1, d)$-protocol (i.e. a uniform tight frame of m vectors) then $\{V_i\}_i \in \mathcal{C}(m, 1, d)$ and*

$$e_2^\psi(V) \geq \psi\left(\left(\frac{d}{m} + c_{m,1,d}, \frac{d}{m} - c_{m,1,d} \right) \right). \tag{28}$$

If we further have that $V_i V_j^* = c_{m,1,d} \, q_{ij}$ for $q_{ij} \in \mathbb{C}$ with $|q_{ij}| = 1$, for every $i \neq j$ then equality holds in (28). Moreover, the converse is true for 2-strongly strict compatible u.i.n.

(ii) *If $\{V_i\}_i$ is a u.w.p. rank-l $(2, l, d)$-protocol then $\{V_i\}_i \in \mathcal{C}(2, l, d)$ and*

$$e_2^\psi(V) \geq \psi\left(\left(\frac{d}{2l} + c_{2,l,d} \right) \mathbf{e}_l, \left(\frac{d}{2l} - c_{2,l,d} \right) \mathbf{e}_l \right).$$

If $\{V_i\}_i$ is a u.w.p-$(2, l, d)$ protocol such that for $i \neq j$, $V_i V_j^* = c_{2,l,d} Q_{ij}$ for unitary operators Q_{ij} in $\mathcal{K}$, it attains the bound for e_2^ψ above.

Proof. By setting respectively $l = 1$, respectively $m = 2$, in (24) we see that in these cases $\mathcal{C}(m, l, d)$ coincides with the class of all u.w.p. rank-l (m, l, d)-protocols (i.e., the condition in the definition of $\mathcal{C}(m, l, d)$ becomes trivial in these cases) so the first part of item (i) and item (ii) follow from Theorem 4.3.

In order to prove the second assertion in item (i) assume that $\| \cdot \|$ is a 2-strongly strict compatible u.i.n. Note that if $\alpha, \beta \in \mathbb{R}^2$ are such that $\mathrm{tr}(\alpha) = \mathrm{tr}(\beta)$ then these vectors are comparable with respect to majorization; indeed $\alpha \prec \beta$ if and only if $\max\{\alpha_1, \alpha_2\} \leq \max\{\beta_1, \beta_2\}$. Assume now that $\| \cdot \|$ is a 2-strongly strict norm and that $\{V_i\}_i$ is an u.w.p. $(m, 1, d)$-protocol in which the lower bound in (28) is attained. Hence, by inspection of the proof of Theorem 4.3 (note that $V_i V_j^* \in \mathbb{C}$ for $l = 1$) we see that if $i \neq j$ then

$$\psi\left(\frac{d}{m} + |V_i V_j^*|, \frac{d}{m} - |V_i V_j^*| \right) \leq \psi\left(\frac{d}{m} + c_{m,1,d}, \frac{d}{m} - c_{m,1,d} \right),$$

which implies that

$$\frac{d}{m} + |V_i V_j^*| \leq \frac{d}{m} + c_{m,1,d} \Rightarrow |V_i V_j^*| \leq c_{m,1,d} \; i \neq j. \tag{29}$$

Since

$$\mathrm{tr}(VV^*) = \mathrm{tr}((VV^*)^2) = \sum_{i \neq j} |V_i V_j^*|^2 + \frac{d^2}{m} = \sum_{i \neq j} c_{m,1,d}^2 + \frac{d^2}{m}$$

we conclude that equality holds in the right hand side of (29) and the theorem follows from this last fact. □

Remark 4.7. The first item in Theorem 4.6 generalizes the results in [8,19] about the optimality of 2-uniform frames to the context of strongly strict compatible unitarily invariant norms.

5. Existence of optimal protocols for one package lost and the q-fundamental inequalities

In [6,8,19,7,33], several examples of 2-loss optimal protocols, i.e., u.w.p. rank-l (m,l,d)-protocols $\{V_i\}$ for which $V_i V_j^* = c_{m,l,d} Q_{ij}$ with $Q_{ij} \in \mathcal{U}(l)$, are constructed based on different techniques. Still, the problem of finding necessary and sufficient conditions for the existence of 1-loss optimal protocols, i.e., u.w.p. rank-l (m,l,d)-protocols, has been considered open (see the discussion in [7] about this topic).

In the case $l = 1$ (i.e., the classical case of frames), the existence of tight normalized frames with given norms of the frame vectors (and hence of 1-loss optimal protocols) is characterized completely by the so-called *fundamental frame inequality* discovered in [11]. Moreover it is now known [2,12,26,29] that the fundamental frame inequality is a particular case of a majorization relation (via the Schur–Horn theorem, see [3,16,21,22,23]) that constitutes a necessary and sufficient condition for the existence of a frame with prescribed norms of the frame vectors and frame operator.

In what follows we exhibit necessary and sufficient (spectral) conditions for the existence of (m,l,d)-protocols $\{V_i\}_i$ with prescribed eigenvalue vectors $\lambda(V_i^* V_i) \in \mathbb{R}^d_{\geqslant 0}$ for $1 \leqslant i \leqslant m$. As in the classical case $l = 1$ there exists a relation between these conditions and an extended notion of (block) majorization as introduced in [28] (via a non-commutative Schur–Horn theorem).

Theorem 5.1. Let $\lambda_i = \lambda_i^\downarrow \in \mathbb{R}^l_{\geqslant 0}$ for $1 \leqslant i \leqslant m$. Then, the following statements are equivalent:

(i) There exists an (m,l,d)-protocol $\{V_i\}_{i=1}^m$ such that $\lambda(V_i^* V_i) = (\lambda_i, 0_{d-l})$, for $1 \leqslant i \leqslant m$.

(ii) There exist $\{A_i\}_{i=1}^m \subset M_d(\mathbb{F})^+$ such that

$$\lambda(A_i) = (\lambda_i, 0_{d-l}) \quad \text{for } 1 \leqslant i \leqslant m \quad \text{and} \quad \sum_{i=1}^m A_i = I_d.$$

(iii) The $(m+1)$-tuple

$$((\lambda_1, 0_{d-l}), \ldots, (\lambda_m, 0_{d-l}), \mathbf{e}) \in (\mathbb{R}^d)^{(m+1)}$$

satisfy Horn–Klyachko's compatibility inequalities plus $\sum_{i=1}^m \operatorname{tr}(\lambda_i) = d$.

(vi) There exists an orthogonal projection $P \in M_m(M_l(\mathbb{F}))$ with $\operatorname{tr}(P) = d$ and such that, if $P = (P_{ij})_{i,j=1}^m$ with $P_{ij} \in M_l(\mathbb{F})$ for $1 \leqslant i,j \leqslant m$, then

$$\lambda(P_{ii}) = \lambda_i \text{ for } 1 \leqslant i \leqslant m.$$

Proof. Clearly, (i) implies (ii) by considering $A_i = V_i^* V_i$ for $1 \leqslant i \leqslant m$. Assume then item (ii). In this case note that $\operatorname{rank}(A_i) \leqslant l$ and hence there exist linear operators $V_i : \mathcal{H} \to \mathcal{K}$ such that $V_i^* V_i = A_i$ for $1 \leqslant i \leqslant m$. It is clear that $\{V_i\}_{i=1}^m$ is an (m,l,d)-protocol as in (i). Therefore, (i) and (ii) are equivalent. The equivalence of items (ii) and (iii) is Theorem 2.7.

Assume again (i) holds and let $V : \mathcal{H} \to \oplus_{i=1}^m \mathcal{K}$ be the analysis operator of the protocol $\{V_i\}_i$. Since $V^* V = \sum_{i=1}^m V_i^* V_i = 1_d$ then we get that the block matrix $VV^* = (V_i V_j^*)_{i,j=1}^m \in M_m(M_l(\mathbb{F}))$ (i.e., the Grammian of $\{V_i\}_i$) is an orthogonal projection; moreover, note that $\operatorname{tr}(VV^*) = \operatorname{tr}(V^* V) = d$ and that the diagonal blocks of the Grammian satisfy $(\lambda(V_i V_i^*), 0_{d-l}) = \lambda(V_i^* V_i) = (\lambda_i, 0_{d-l})$, for $1 \leqslant i \leqslant m$ (see the comments after Definition 2.4). Conversely, assume that item (iv) holds and let $V : \mathcal{H} \to \oplus_{i=1}^m \mathcal{K}$ be an isometry such that $VV^* = P$ (such an isometry exists since $\operatorname{rank}(P) = d$ by assumption). Let $V_i : \mathcal{H} \to \mathcal{K}$ for $1 \leqslant i \leqslant m$ be such that $Vx = \oplus_{i=1}^m V_i x$ and note that then $P = VV^* = (V_i V_j^*)_{ij}$ and that $I_d = V^* V = \sum_{i=1}^m V_i^* V_i$ that is, $\{V_i\}_i$ is an (m,l,d)-protocol as in (i). Thus, items (i) and (iv) are equivalent. □

Remark 5.2. Using the characterization in item (iv) in Theorem 5.1 and the reduction described in [27] (which is relevant from an algorithmic point of view) it is possible to show that Horn–Klyachko's compatibility inequalities in (iii) in Theorem 5.1 can be reduced to a system of inequalities that, in case $l = 1$ are simply the conditions given in the majorization relation $\mathrm{diag}(\|P_{11}\|^2, \ldots, \|P_{mm}\|^2) \prec I_d \oplus \mathbf{0}_{m \cdot l - d}$, where $\mathrm{diag}(x) \in M_n(\mathbb{C})$ is the diagonal matrix with main diagonal $x \in \mathbb{C}^n$.

Actually, the inequalities in (iii) in Theorem 5.1 can be regarded as determining an extended notion of majorization as defined in [28]. Indeed, with the terminology of [28, Definition 4.4], the conditions given in Theorem 5.1 are also equivalent to the **t**-extended majorization relation $\bigoplus_{i=1}^m \mathrm{diag}(\lambda_i) \prec_{\mathbf{t}} I_d \oplus \mathbf{0}_{m \cdot l - d} \in M_{m \cdot l}(\mathbb{C})$, where $t = (\mathbf{e}_l, 1)_{i=1}^m$.

Corollary 5.3 (q-fundamental projective (m, l, d)-protocol inequalities). *Let $t(i) \in \{1, \ldots, l\}$ and $w_i \in \mathbb{R}_{> 0}$ for $1 \leqslant i \leqslant m$. Then, there exists a projective (m, l, d)-protocol $\{V_i\}_{i=1}^m$ for the Hilbert space $\mathcal{H}$ such that $V_i^* V_i = w_i P_i$ for orthogonal projections P_i with $\mathrm{tr}(P_i) = t(i)$ for $1 \leqslant i \leqslant m$ if and only if for every $1 \leqslant r \leqslant d$ and every $(J_0, \ldots, J_m) \in LR_r^d(m)$ we have that*

$$r \leqslant \sum_{i=1}^m w_i \cdot |J_i \cap \{1, \ldots, t(j)\}|$$

plus the condition $d = \sum_{i=1}^m w_i \cdot t(i)$.

As an immediate consequence of the *q*-f.p.p.i. we conclude that u.w.p. rank-*l* (m, l, d)-protocols exist if and only if for every $1 \leqslant r \leqslant d$ and every $(J_0, \ldots, J_m) \in LR_r^d(m)$ it holds that

$$r \leqslant \frac{d}{m \cdot l} \cdot \sum_{i=1}^m |J_i \cap \{1, \ldots, l\}|.$$

It turns out that Corollary 5.3 plays a central role in the study of the fusion frame potential recently considered in [30]. In particular, Horn–Klyachko's inequalities allow the study and description of the spectral structure of (local) minimizers of this functional defined for fusion frames in finite dimensional Hilbert spaces.

Example 5.4. Next, we show explicitly how to construct a projection $P = (P_{ij})_{ij} \in M_m(M_l(\mathbb{C}))$ such that $P_{ii} = \frac{d}{m \cdot l} I$ for $1 \leqslant i \leqslant m$, when $d = k \cdot l$ for some $k \in \mathbb{N}$. Thus, by Theorem 5.1, we show the existence of u.w.p. rank-*l* (m, l, d)-protocols in this case. This construction is a particular case of that appearing in the proof of [28, Proposition 4.12]: consider first $\xi \in \mathbb{C}$ an *m*th primitive root of unity and let $\widetilde{U} \in \mathcal{M}_m(\mathbb{C})$ be the matrix with *j*th row given by

$$R_j(\widetilde{U}) = 1/\sqrt{m}\,(1, \xi^j, \xi^{2j}, \ldots, \xi^{(m-1)j}), \quad 1 \leqslant j \leqslant m.$$

It is then straightforward to show that the rows of $\widetilde{U}$ form an orthonormal basis for $\mathbb{C}^m$ and hence $\widetilde{U} \in \mathcal{U}(m)$ is a unitary matrix. Let $U \in \mathcal{U}(d \cdot m)$ be the block matrix $U = (\widetilde{U}_{ij} \cdot 1_d)_{i,j=1}^m$. Then, consider the matrix $A = \bigoplus_{i=1}^k I = (A_{ij})_{ij} \oplus \mathbf{0}_{(m-k)l} \in M_m(M_l(\mathbb{C}))$ and note that

$$U^* A U = (P_{ij})_{ij}, \quad P_{ii} = \frac{1}{m} \sum_{i=1}^m A_{ii} = \frac{k}{m} I,$$

where the last equality follows from the diagonal block structure of A and by construction of U. Now, recall that $k = \frac{d}{l}$ and we are done.

Acknowledgments

regarding the material in this note. I would also like to acknowledge the anonymous referee for suggesting the content of Remark 3.5 (for the cases of the spectral and operator norm).

References

[1] T. Ando, Majorization, Doubly Stochastic Matrices and Comparison of Eigenvalues, Lecture Notes, Hokkaido University, 1982.
[2] J. Antezana, P. Massey, M. Ruiz, D. Stojanoff, The Schur–Horn theorem for operators and frames with prescribed norms and frame operator, Illinois J. Math., 51 (2) (2007) 537–560.
[3] W. Arveson, R.V. Kadison, Diagonals of self-adjoint operators, Oper. Theory, Oper. Algebras Appl., Amer. Math. Soc., Providence, RI, Contemp. Math. 414 (2006) 247–263.
[4] J.J. Benedetto, M. Fickus, Finite normalized tight frames, Adv. Comput. Math. 18 (2003) 357–385.
[5] R. Bhatia, Matrix Analysis, Graduate Texts in Mathematics, vol. 169, Springer-Verlag, New York, 1997.
[6] B.G. Bodmann, Optimal linear transmission by loss-insensitive packet encoding, Appl. Comput. Harmon. Anal. 22 (3) (2007) 274–285.
[7] B.G. Bodmann, D.W. Kribs, V.I. Paulsen, Decoherence-insensitive quantum communication by optimal C^*-encoding, IEEE Trans. Inform. Theory 53 (2007) 4738–4749.
[8] B.G. Bodmann, V.I. Paulsen, Frames, graphs and erasures, Linear Algebra Appl. 404 (2005) 118–146.
[9] P.G. Casazza, The art of frame theory, Taiwanese J. Math. 4 (2) (2000) 129–201.
[10] M. Fickus, B.D. Johnson, K. Kornelson, K.A. Okoudjou, Convolutional frames and the frame potential, Appl. Comput. Harmon. Anal. 19 (2005) 77–91.
[11] P.G. Casazza, M. Fickus, J. Kovacevic, M.T. Leon, J.C. Tremain, A physical interpretation for tight frames, harmonic analysis and applications, Appl. Numer. Harmon. Anal. (2006) 51–76.
[12] P.G. Casazza, M.T. Leon, Frames with a given frame operator, preprint.
[13] P.G. Casazza, J. Kovacevic, Equal-norm tight frames with erasures, Adv. Comput. Math. 18 (2003) 387–430.
[14] P.G. Casazza, G. Kutyniok, Frames of subspaces, in: Wawelets, Frames and Operator Theory, Amer. Math. Soc., Providence, RI, Contemp. Math. 345 (2004) 87–113.
[15] P.G. Casazza, G. Kutyniok, S. Li, Fusion frames and distributed processing, Appl. Comput. Harmon. Anal. 25 (1) (2008) 114–132.
[16] K. Dykema, D. Freeman, K. Kornelson, D. Larson, M. Ordower, E. Weber, Ellipsoidal tight frames and projection decompositions of operators, Illinois J. Math. 48 (2) (2004) 477–489.
[17] W. Fulton, Young Tableaux. With Applications to Representation Theory and Geometry, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997.
[18] W. Fulton, Eigenvalues, invariant factors, highest weights, and Schubert calculus, Bull. Amer. Math. Soc. (N.S.) 37 (3) (2000) 209–249.
[19] R.B. Holmes, V.I. Paulsen, Optimal frames for erasures, Linear Algebra Appl. 377 (2004) 31–51.
[20] R.A. Horn, C.R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, Corrected reprint of the 1985 original.
[21] R.V. Kadison, The Pythagorean theorem. I. The finite case, Proc. Natl. Acad. Sci. USA 99 (7) (2002) 4178–4184.
[22] R.V. Kadison, The Pythagorean theorem. II. The infinite discrete case, Proc. Natl. Acad. Sci. USA 99 (8) (2002) 5217–5222.
[23] V. Kaftal, G. Weiss, A survey on the interplay between arithmetic mean ideals, traces, lattices of operator ideals, and an infinite Schur–Horn majorization theorem, Hot topics in operator theory, Theta, Bucharest, Theta Ser. Adv. Math. 9 (2008) 101–135.
[24] A. Klyachko, Stable bundles, representation theory and Hermitian operators, Selecta Math. (N.S.) 4 (3) (1998) 419–445.
[25] A. Knutson, T. Tao, The honeycomb model of $GL_n(C)$ tensor products. I. Proof of the saturation conjecture, J. Amer. Math. Soc. 12 (4) (1999) 1055–1090.
[26] K.A. Kornelson, D.R. Larson, Rank-one decomposition of operators and construction of frames, in: Wavelets, Frames and Operator Theory, Amer. Math. Soc., Providence, RI, Contemp. Math. 345 (2004) 203–214.
[27] C.K. Li, Y.T. Poon, Principal submatrices of a Hermitian matrix, Linear and Multilinear Algebra 51 (2) (2003) 199–208.
[28] P. Massey, Non-commutative Schur–Horn theorems and extended majorization for hermitian matrices, Linear and Multilinear Algebra, in press.
[29] P. Massey, M. Ruiz, Minimization of convex functionals over frame operators, Avd. Comput. Math., in press.
[30] P. Massey, M. Ruiz, D. Stojanoff, The structure of minimizers of the frame potential on fusion frames, submitted for publication. arXiv:0811.3159.
[31] Rotfel'd, S. Ju, The singular values of the sum of completely continuous operators, in: Problems of Mathematical Physics, Izdat. Leningrad. University (3) (1968) 81–87.
[32] T. Strohmer, R.W. Heath Jr., Grassmannian frames with applications to coding and communication, Appl. Comput. Harmon. Anal. 14 (2003) 257–275.
[33] J.A. Tropp, I.S. Dhillon, R.W. Heath Jr., T. Strohmer, Designing structured tight frames via alternating projection, IEEE Trans. Inform. Theory 51 (1) (2005) 188–209.
[34] L. Welch, Lower bounds on the maximum cross correlation of signals, IEEE Trans. Inform. Theory 20 (3) (1974) 397–399.