Mutually unbiased measurements in finite dimensions

Amir Kalev and Gilad Gour

1 Center for Quantum Information and Control, University of New Mexico, Albuquerque, NM 87131-0001, USA
2 Institute for Quantum Science and Technology, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
E-mail: amirk@unm.edu

Received 30 January 2014
Accepted for publication 8 April 2014
Published 21 May 2014

New Journal of Physics 16 (2014) 053038
doi:10.1088/1367-2630/16/5/053038

Abstract

We generalize the concept of mutually unbiased bases (MUB) to measurements which are not necessarily described by rank one projectors. As such, these measurements can be a useful tool to study the long-standing problem of the existence of MUB. We derive their general form, and show that in a finite, $d$-dimensional Hilbert space, one can construct a complete set of $d+1$ mutually unbiased measurements. Besides their intrinsic link to MUB, we show that these measurements’ statistics provide complete information about the state of the system. Moreover, they capture the physical essence of unbiasedness, and in particular, they satisfy a non-trivial entropic uncertainty relation similar to $d+1$ MUB.

Keywords: mutually unbiased measurements, mutually unbiased bases, entropic uncertainty relations

Unbiased bases are a fundamental concept in the theory of quantum kinematics, as they are intimately related to Bohr’s Complementarity Principle [1]. In a finite dimensional Hilbert space, two orthonormal bases are said to be unbiased if, and only if, the transition probability from any state of one basis to any state of the second basis is constant. In a $d$-dimensional Hilbert space there are at most $d+1$ bases which are pairwise unbiased [2]. This set is called the set of mutually unbiased bases (MUB).

MUB are studied in various contexts in quantum mechanics. They are used in thought experiments such as the so-called ‘mean king problem’ [3, 4], in which they were shown to
have interesting connections with symmetric informationally complete positive-operator-valued measures [5], complex $t$-designs [6, 7], and graph state formalism [8]. Beyond being of fundamental interest, MUB have practical importance as well. They play an important role in quantum error correction codes [9, 10], quantum cryptography for secure quantum key exchange [11, 12], quantum state tomography [13, 14], and more recently in the detection of quantum entanglement [15].

Therefore, there has been of great effort and research interest in constructing the complete set of MUB. To date, numerous construction methods of complete sets of MUB are known in power of prime dimensions [2, 8, 14, 16–19], and each method provides a useful and different insight for the problem of the existence of MUB. Alas, it is still not known whether complete sets of MUB exist in all finite dimensions. A strong numerical evidence suggests that they do not exist in dimensions which are not power of prime [20–23].

In this work we propose a new approach for ‘unbiasedness,’ by generalizing this notion from bases to measurements. More particularly, we consider unbiased measurements in a $d$-dimensional Hilbert space, such that unbiased bases are a special, limiting case. In fact, this idea enables us to construct all possible complete sets of $d + 1$ mutually unbiased measurements (MUM) in a $d$-dimensional Hilbert space. Therefore, if a complete set of MUB exists, it must be a particular case of this construction. Naturally, this generalization can be useful to study questions relevant to MUB. One interesting question, for example, is how close $d + 1$ MUM can get to a complete set of MUB in a given dimension—say, in dimension 6. Besides their relevance to MUB, MUM may be of interest on their own. We show that they provide a linear inversion formula for quantum state tomography, and that they abide by entropic uncertainty relations, similar to MUB.

In order to formulate the notion of MUM, we first briefly recall the measurement formalism in quantum mechanics. Generally, a measurement in quantum mechanics is described by a set of positive operators (sometimes called measures) $M_j \geq 0$ that sum to the identity operator, $\sum_j M_j = 1$. The probability of the $j$th outcome is given by Born’s rule, $\text{Tr}(M_j \rho)$, where $\rho$ is the state (statistical operator) of the quantum system. This representation of a measurement is therefore called a probability-operator measurement (POM), or equivalently a positive-operator-valued measure (POVM).

Clearly a basis of a finite-dimensional Hilbert space defines both a set of states and a measurement. In particular, consider a set of $d + 1$ MUB in a $d$-dimensional Hilbert space, $\left\{ |\psi_n^{(b)}\rangle \right\}$ where $b = 1, 2, \ldots, d + 1$ labels the basis while $n = 1, 2, \ldots, d$ labels the vectors within a basis. The set of projectors on the $b$th basis vectors, $\{ G_n^{(b)} = B_n^{(b)} = |\psi_n^{(b)}\rangle \langle \psi_n^{(b)}|, n = 1, 2, \ldots, d \}$, form a measurement, $B_n^{(b)} \geq 0$, and $\sum_n B_n^{(b)} = 1$, $\forall b$, with the defining properties of MUB,

\[
\text{Tr} \left( B_n^{(b)} \right) = 1, \\
\text{Tr} \left( B_n^{(b)} B_n^{(b')} \right) = \delta_{n,n'} \delta_{b,b'} + \left( 1 - \delta_{b,b'} \right) \frac{1}{d}.
\] (1)
The $B_{n}^{(b)}$ can be thus regarded as quantum states and as measurement operators. Therefore, the unbiasedness of two bases could be re-stated as a property of two measurements as follows: In a $d$-dimensional Hilbert space, measurements of two bases are unbiased if, and only if, when the system is in any state of one basis (measurement), the probability distribution upon measuring it in the second measurement is completely random.

The notion of unbiasedness of measurements of bases can be therefore generalized to general measurements.

**Definition 1.** Two measurements on a $d$-dimensional Hilbert space, $\mathcal{P}^{(b)} = \left\{ P_{n}^{(b)} \mid P_{n}^{(b)} \geq 0, \sum_{n=1}^{d} P_{n}^{(b)} = 1 \right\}$, $b = 1, 2$, with $d$ elements each, are said to be mutually unbiased measurements (MUM) if, and only if,

\[
\begin{align*}
\text{Tr} \left( P_{n}^{(b)} \right) &= 1, \\
\text{Tr} \left( P_{n}^{(b)} P_{n'}^{(b')} \right) &= \delta_{n,n'} \delta_{b,b'} \kappa + \left( 1 - \delta_{n,n'} \right) \delta_{b,b'} \frac{1 - \kappa}{d - 1} \\
&\quad + \left( 1 - \delta_{b,b'} \right) \frac{1}{d}.
\end{align*}
\]

(2)

According to this definition, each measurement operator $P_{n}^{(b)}$ can be also regarded as a quantum state, for which $\text{Tr} \left( P_{n}^{(b)} P_{n'}^{(b')} \right) = 1/d$, $\forall b \neq b'$. Therefore, indeed, if the system is in any state, say of $\mathcal{P}^{(1)}$, then the probability distribution of measuring it in a second measurement, say $\mathcal{P}^{(2)}$, is completely random ($1/d$).

The inner product of two elements within the same measurement depends on the efficiency parameter $\kappa$. The value of this parameter determines how close the measurements operators are to rank one projectors, i.e., to MUB. The latter is obtained for $\kappa = 1$. The other extreme is $\kappa = \frac{1}{d}$, which corresponds to the trivial case where all the measurement operators are equal to the completely mixed state. We therefore conclude that the efficiency parameter satisfies, $\frac{1}{d} < \kappa \leq 1$.

Before moving on, we note that, within this definition, the purity of each state (that is, of the measurement operator) $P_{n}^{(b)}$ is a constant equal to $\kappa$. One may consider more general definitions of MUM in which the purity of the states depends, for example, on the measurement label $b$ and on the outcome label $n$, $\kappa_{n}^{(b)}$. These definitions, however, result in less symmetric MUM, which are the primary objective of our study.

---

3 Consider a measurement in a $d$-dimensional Hilbert space, such that the inner product between two measurement elements is given by $\text{Tr} \left( M_{i} M_{j}^{*} \right) = \kappa \delta_{i,j} + \left( 1 - \delta_{i,j} \right) \gamma$. The two parameters, $\kappa$ and $\gamma$ depend on each other. Indeed from $\sum_{i,j} \text{Tr} \left( M_{i} M_{j}^{*} \right) = d$ we obtain $\gamma = \frac{1 - \kappa}{d - 1}$. Moreover, $\kappa$ is bounded from below:

$1 = \text{Tr} \left( M_{i} \right) \leq \sqrt{\text{Tr} \left( M_{j} M_{j}^{*} \right) \text{Tr} \left( 1 \right)} = \sqrt{\kappa d}$, implies that $1/d \leq \kappa$. Since the largest value of $\kappa$ is 1, we get $1/d < \kappa \leq 1$. 

---
The definition above allows us to construct $d + 1$ MUM in a $d$-dimensional Hilbert space. Consider an orthogonal basis, $F_k$, for the space of hermitian, traceless operators acting on a $d$-dimensional Hilbert space. Such a basis is composed of $d^2 - 1$ operators, $F_k = F_k^\dag$, satisfying $\text{Tr} (F_k) = 0$, and $\text{Tr} (F_k F_l) = \delta_{k,l}$. We arrange the basis elements on a grid of $d - 1$ columns and $d + 1$ rows,

$$
\begin{array}{cccccc}
F_1 & F_2 & \cdots & F_{d-1} \\
F_d & F_{d+1} & \cdots & F_{2(d-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\cdots & \cdots & \cdots & F_{(d+1)(d-1)}.
\end{array}
$$

(3)

It is convenient to re-label the operators by a double index $(n,b)$ according to their (column, row) location $n = 1, 2, \ldots, d - 1$, $b = 1, 2, \ldots, d + 1$,

$$
\begin{array}{cccccc}
F_{1,1} & F_{2,1} & \cdots & F_{d-1,1} \\
F_{1,2} & F_{2,2} & \cdots & F_{d-1,2} \\
\vdots & \vdots & \ddots & \vdots \\
F_{1,d+1} & F_{2,d+1} & \cdots & F_{d-1,d+1}.
\end{array}
$$

(4)

Next, we define the $d (d + 1)$ operators

$$
F_n^{(b)} = \begin{cases} 
F_n^{(b)} - (d + \sqrt{d})F_{n,b} & \text{for } n = 1, 2, \ldots, d - 1 \\
(1 + \sqrt{d})F_n^{(b)} & \text{for } n = d
\end{cases}
$$

(5)

with $b = 1, 2, \ldots, d + 1$, and $F_n^{(b)}$ being the sum of the basis elements on the $b$th row, i.e., $F_n^{(b)} = \sum_{n=1}^{d-1} F_{n,b}$. This definition ensures the properties,

$$
\text{Tr} \left( F_n^{(b)} F_n^{(b)} \right) = \left( 1 + \sqrt{d} \right)^2 \left[ \delta_{nn'} (d - 1) - (1 - \delta_{nn'}) \right],
$$

$$
\sum_{n=1}^d F_n^{(b)} = 0,
$$

(6)

which will be used later. We note in passing that, by construction

$$
\text{Tr} \left( F_n^{(b)} F_n^{(b')} \right) = 0, \ \forall \ b \neq b', \ \forall \ n, n' = 1, 2, \ldots, d.
$$

(7)

**Theorem 1.** The operators,

$$
P_n^{(b)} = \frac{1}{d} + t F_n^{(b)},
$$

(8)

with $b = 1, 2, \ldots, d + 1$, $n = 1, 2, \ldots, d$, and the free parameter $t$ chosen such that $P_n^{(b)} \geq 0$, form $d + 1$ MUM in a $d$-dimensional Hilbert space, where $b$ labels the measurement and $n$ labels the outcome. Moreover, any complete set of MUM has this form.
**Proof.** To show that the $P_n^{(b)}$ of equation (8) form MUM, one can verify that they satisfy the definition of MUM, equation (2), with efficiency parameter

$$\kappa = \frac{1}{d} + t^2 \left(1 + \sqrt{d}\right)^2 (d - 1). \tag{9}$$

Conversely, to prove that all MUM have the structure of equation (8), we assume that the $P_n^{(b)}$ form $d + 1$ MUM according to definition 1 and show that they have the form of equation (8) where the $F_n^{(b)}$ form an orthonormal hermitian operator basis. By their definition the $P_n^{(b)}$ are both quantum states and form $d + 1$ MUM; hence we can write them, without loss of generality, in the form of equation (8), where $t$ is independent of the indices $n$ and $b$, and is related to $\kappa$ by equation (9). Next, we can always cast the (hermitian traceless) operators $F_n^{(b)} = (P_n^{(b)} - \frac{1}{d})/t$, satisfying equations (6) and (7), in the form of equation (5). It remains to prove that the $F_n^{(b)}$ of equation (5) form an orthonormal hermitian operator basis. This could be verified by using the properties of the $P_n^{(b)}$.

The efficiency parameter, given in equation (9), obtains its maximal value $\kappa = 1$ for $t^2 \left(1 + \sqrt{d}\right)^2 = \frac{1}{d}$. In this case the MUM are actually MUB. Clearly, the efficiency parameter is determined by the free parameter $t$, which in turn is set such that $P_n^{(b)} \geq 0$. This requirement implies that the range of $t$ is

$$-\frac{1}{d \lambda_{\max}} \leq t \leq \frac{1}{d |\lambda_{\min}|} \tag{10}$$

where $\lambda_{\min} = \min \lambda_{\min}^{(b)}$, $\lambda_{\max} = \max \lambda_{\max}^{(b)}$, and $\lambda_{\min}^{(b)}$ and $\lambda_{\max}^{(b)}$ are the smallest (negative) and largest (positive) eigenvalues of the operators $F_n^{(b)}$ of equation (5) with $n = 1, 2, \ldots, d$, respectively. (Since $\text{Tr} \left( F_n^{(b)} \right) = 0$, these operators must have both negative and positive eigenvalues.) The larger the $t$, in its magnitude, the larger the efficiency parameter would eventually be. Therefore we define the optimal $t$ to be

$$t_{opt} = \begin{cases} \frac{1}{d \lambda_{\min}} & \text{for } |\lambda_{\min}| < \lambda_{\max}, \\ -\frac{1}{d \lambda_{\max}} & \text{for } \lambda_{\max} < |\lambda_{\min}|. \end{cases} \tag{11}$$

The optimal efficiency parameter of a MUM is given by $\kappa_{opt} = \frac{1}{d} + t_{opt}^2 \left(1 + \sqrt{d}\right)^2 (d - 1)$. This choice of $t_{opt}$ ensures $P_n^{(b)} \geq 0 \ \forall \ b$ and $n$. The value of $t_{opt}$ depends on the particular choice of the operator basis $F_n^{(b)}$. For a given choice, $\kappa_{opt}$ sets an upper bound on how close we can get to MUB. The question of whether a complete set of MUB exists in any finite dimension is then translated to the question whether there exists an operator basis for which $\kappa_{opt} = 1$. In appendix A we show that for the case where the traceless hermitian operator basis is the generalized Gell-Mann operator basis, an optimal efficiency parameter can be analytically calculated,
\[ \kappa_{\text{opt}} = \frac{1}{d} + \frac{2}{d^2}. \]

In a sense, the Gell-Mann operator basis is not a good choice for a basis, since the optimal efficiency parameter is very close to its minimal value \( \frac{1}{d} \) (except for \( d = 2 \), for which it equals 1). Of course, one may resort to numerical methods to estimate a better value of \( \kappa_{\text{opt}} \) in a given dimension.

The MUM share various properties with MUB. For example, the set of the \( d + 1 \) MUM of equation (2) are informationally complete, that is, any state of the system is determined completely by the MUM outcomes’ probabilities, \( p_n^{(b)} = \text{Tr} \left( P_n^{(b)} \rho \right) \). In fact, much like MUB, the MUM provide a linear inversion relation,

\[ \rho = \sum_{n,b} p_n^{(b)} R_n^{(b)}, \]  

where the reconstruction operators \( R_n^{(b)} \) associated with the MUM are linear functions of the outcomes \( P_n^{(b)} \),

\[ R_n^{(b)} = \frac{d - 1}{\kappa d - 1} \left( p_n^{(b)} - \frac{d - \kappa}{d^2 - 1} \right). \]  

The reconstruction operators satisfy their defining property,

\[ \text{Tr} \left( \rho P_n^{(b)} \right) = \sum_{n,b} p_n^{(b)} \text{Tr} \left( R_n^{(b)} P_n^{(b)} \right) = p_n^{(b)}. \]  

In appendix B we consider a measurement related to MUM with \( d^2 \) outcomes which, as well, provides a linear inversion formula for quantum state tomography.

Beyond the mathematical generalization of MUB, the MUM have a physical significance of their own. As discussed above, the MUM elements, \( P_n^{(b)} \) of equation (8), can be regarded as quantum states, and the outcome of measuring a state of one measurement in any other MUM, is completely random. We now formalize this aspect of complementarity of the MUM by showing that they satisfy a non-trivial entropic uncertainty relation similar to the one satisfied by MUB. When the latter exist, they satisfy the strong entropic uncertainty relation [24, 25],

\[ \frac{1}{d + 1} \sum_{b=1}^{d+1} H \left( \mathcal{B}^{(b)}, \rho \right) \geq \log \frac{d + 1}{2}, \]  

where \( H \left( \mathcal{B}^{(b)}, \rho \right) = -\sum_{n=1}^d p_n^{(b)} \log p_n^{(b)} \) is the Shannon entropy of the probability distribution, \( p_n^{(b)} = \langle \psi_n^{(b)} | \rho | \psi_n^{(b)} \rangle \), associated with measuring the system \( \rho \) in MUB measurement

\[ \mathcal{B}^{(b)} = \left\{ | \psi_n^{(b)} \rangle \langle \psi_n^{(b)} | n = 1, 2, \ldots, d \right\}. \]

**Theorem 2.** The complete set of \( d + 1 \) MUM \( \{ \mathcal{P}^{(b)} \} \) of equation (8) in a \( d \)-dimensional Hilbert space, satisfies the entropic uncertainty relation,

\[ \frac{1}{d + 1} \sum_{b=1}^{d+1} H \left( \mathcal{P}^{(b)}, \rho \right) \geq \log \frac{d + 1}{\kappa}, \]

where \( \kappa \) is the efficiency parameter.
The proof is given in appendix C. Note that the inequality of equation (15), abide by the MUB, is a particular instance of equation (16) for the maximal value of the parameter efficiency \( \kappa, \kappa = 1 \). The MUM with an optimal efficiency parameter, \( \kappa_{\text{opt}} \), satisfies equation (16) with \( \kappa = \kappa_{\text{opt}} \).

The inequality \( \log \frac{d+1}{1+\kappa} \geq \log \frac{d+1}{2} \) for \( \kappa \in (\frac{1}{d}, 1] \) apparently indicates that the smaller the \( \kappa \) the stronger the inequality. This counterintuitive result can be resolved by noting that for the minimum value of \( \kappa = \frac{1}{d} \), the measurement operators are the completely mixed state, and as such do not provide any information about the state of the system; hence the uncertainty is the largest. This implies that the uncertainty of each measurement must be taken into account before drawing conclusion about the mutual unbiasedness of the MUM. Indeed, there is a distinction between the uncertainty relation of equation (15) satisfied by MUB and the uncertainty relation of equation (16) abide by general MUM. This distinction originates in the difference between a measurement of a basis and a general measurement, such as MUM. To be more precise, let us define a state-dependent uncertainty associated with a measurement \( \mathcal{M} \) as, say, the Shannon entropy of its probability distribution, \( H(\mathcal{M}, \rho) \). Now suppose that \( \mathcal{M} \) is a measurement of a basis. In this case there always exist states—the basis states—for which the state-dependent uncertainty is zero. It is therefore reasonable to define a state-independent uncertainty associated with a measurement as the minimum of the state-dependent measurement uncertainty,

\[
\Delta \mathcal{M} = \min_{\rho} H(\mathcal{M}, \rho). \quad (17)
\]

A measurement has in general an uncertainty \( \Delta \mathcal{M} \) larger than than zero. Going back to the uncertainty relations, we conclude that since the MUB are both measurements with zero uncertainty, the entropic uncertainty relation of equation (15) captures the complementarity, or unbiasedness, aspect of the measurements. In contrast, each one of the MUM is uncertain in general. Therefore, though equation (16) provides an entropic uncertainty relation, it includes the ‘self’ uncertainty of each measurement. To account for the unbiasedness feature of the MUM we must subtract the uncertainty of each measurement,

\[
v = \frac{1}{d+1} \sum_{b=1}^{d+1} \left[ H(\mathcal{P}^{(b)}, \rho) - \Delta \mathcal{P}^{(b)} \right] . \quad (18)
\]

so that the proper complementarity of entropic uncertainty reads

\[
v \geq \log \frac{d+1}{1+\kappa} - \frac{1}{d+1} \sum_{b=1}^{d+1} \Delta \mathcal{P}^{(b)} . \quad (19)
\]

Certain techniques, for example, those introduced in [26], may be used to calculate \( \Delta \mathcal{P}^{(b)} \). We have numerically searched for \( \Delta \mathcal{P}^{(b)} \) for the case where the MUM are constructed by the generalized Gell-Mann operator basis as given in appendix A. Searching over \( 10^6 \) states in six-dimensional Hilbert space of random rank, we found that the MUM satisfy a non-trivial complementarity relation, as described in figure 1 and its caption.

To conclude, in this work we generalized the notion of unbiasedness of bases, MUB, to general measurements, MUM. We constructed the complete set, i.e., \( d+1 \) MUM in a \( d \)-dimensional Hilbert space, where MUB, when they exist, are a particular case thereof.
This construction can be used to study, either analytically or numerically, the problem of the existence of MUB in non-power-of-prime dimensions, and may be helpful to obtain bounds on how close we can get to MUB in these cases. We showed that this mathematical generalization captures the physical essence of unbiased bases in two principal aspects. First, the probability of obtaining any outcome upon preparing the system in one of the $d$ measurement elements, and measuring it in the other measurement, is independent of the prepared state and the measurement outcome. Second, a complete set of MUM satisfies a non-trivial entropic uncertainty relation, similar to MUB. Moreover, this relation answers an interesting question regarding the existence of an entropic uncertainty relation among $d + 1$ measurement settings in finite $d$-dimensional Hilbert space [25].

**Acknowledgments**

AK’s research is supported by NSF Grant PHY-1212445. GG’s research is supported by NSERC.

**Appendix A. Optimal efficiency parameter for the case of the generalized Gell-Mann operator basis**

In this appendix we explicitly calculate the optimal efficiency parameter, $\kappa_{\text{opt}}$, for the case where the operator bases, $F_{n,b}$, are the well-known generalized Gell-Mann (GM) operators (known also as the generalized Pauli operators). For this aim we first consider the range of $j^{(b)}$ making $P_n^{(b)} \geq 0$. 

![Figure 1. Measure of unbiasedness as a function of $\kappa$ for MUM on a six-dimensional Hilbert space constructed from the Gell-Mann operator basis described in appendix A. The range of $\kappa$ plotted is $\frac{3}{4} < \kappa \leq \kappa_{\text{opt}} = \frac{1}{d} + \frac{3}{36}$. For a given $\kappa$ value, the uncertainty of the MUM is larger than the value represented by the dotted line.](image)
The generalized GM operators are a set of \( d^2 - 1 \) operators which form a basis for traceless hermitian operators acting on a \( d \)-dimensional Hilbert space. We can label them by two indexes \( n, m \) each taking on integer values, \( n, m = 1, 2, \ldots, d \), such that

\[
G_{n,m} = \begin{cases} 
\frac{1}{\sqrt{2}} (|n\rangle \langle m| + |m\rangle \langle n|) & \text{for } n < m, \\
\frac{i}{\sqrt{2}} (|n\rangle \langle m| - |m\rangle \langle n|) & \text{for } m < n
\end{cases}
\]  

(A.1)

and for \( n = m \), with \( n = 1, 2, \ldots, d - 1 \),

\[
G_{n,n} = \frac{1}{\sqrt{n(n+1)}} \left( \sum_{k=1}^{n} |k\rangle \langle k| - n|n+1\rangle \langle n+1| \right).
\]  

(A.2)

The constant in equations (A.1) and (A.2) were chosen such that \( \text{Tr} \left( G_{n,m}^2 \right) = 1 \) for all possible \( n \) and \( m \). It is helpful to think of these operators as elements of a \( d \times d \) matrix whose most bottom-right element of the matrix is not ‘populated’ with an operator,

\[
\begin{pmatrix}
G_{1,1} & G_{2,1} & \cdots & G_{d,1} \\
G_{1,2} & G_{2,2} & \cdots & G_{d,2} \\
\vdots & \vdots & \ddots & \vdots \\
G_{1,d} & \cdots & \cdots & [ ]
\end{pmatrix}
\]  

(A.3)

There is a matter of arbitrariness how as to make the correspondence between the \( F \) of equation (4) and the GM operators. We choose here the following correspondence:

\[
\begin{array}{cccccccc}
F_{1,1} & F_{2,2} & \cdots & F_{d-1,d-1} & G_{2,1} & G_{3,1} & \cdots & G_{d,1} \\
F_{2,2} & F_{3,3} & \cdots & F_{d,d} & G_{3,2} & G_{4,2} & \cdots & G_{d,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
F_{d-1,d-1} & F_{d-1,d-1} & \cdots & F_{d,d} & G_{d-1,d-1} & \cdots & \cdots & \cdots \\
\end{array}
\]  

(A.4)

where for the first \( d \) rows of equation (4), we equate the \( F \) on the \( b \)th row with the \( G \) on the \( b \)th row in the matrix of equation (A.3) except the diagonal matrix element. The \( F \) on the last, \( d + 1 \) th, row correspond to diagonal elements \( G_{n,n} \).

Lets now calculate the eigenvalues of \( F_n^{(b)} \), or equivalently, the eigenvalues of \( F^{(b)} \) and \( F^{(b)} - \alpha F_{n,b} \), cf equation (5). Throughout this section we denote \( d + \sqrt{d} \equiv \alpha \), and \( 1 + \sqrt{d} \equiv \beta \). We start with \( F^{(1)} \),

\[
F^{(1)} = \frac{1}{\sqrt{2}} \left( \sum_{j=2}^{d} |j\rangle \langle j| + |\bar{j}\rangle \langle \bar{j}| \right).
\]  

(A.5)
whose $d \times d$ matrix representation is

\[
F^{(1)} = \frac{1}{\sqrt{2}} \begin{pmatrix}
0 & 1 & \cdots & 1 \\
1 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 0 & \cdots & 0
\end{pmatrix}.
\] (A.6)

Its eigenvalues $\lambda$ can be found by the eigenvalues equation

\[
\text{Det} \begin{pmatrix}
-\lambda & 1 & \cdots & 1 \\
\sqrt{2} & -\lambda & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\sqrt{2} & 0 & \cdots & -\lambda
\end{pmatrix} = 0.
\] (A.7)

To solve this equation we use the identity

\[
\text{Det} \begin{pmatrix}
A & B \\
C & D
\end{pmatrix} = \text{Det} (D) \text{Det} (A - BD^{-1}C),
\] (A.8)

which holds for invertible $D$. By identifying,

\[
A = -\lambda, \quad B = \frac{1}{\sqrt{2}} (1, 1, \ldots, 1) = C^i,
\]

\[
D = \begin{pmatrix}
-\lambda & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & -\lambda
\end{pmatrix},
\] (A.9)

we can write the eigenvalues equation, equation (A.7), as

\[
\lambda^{d-2} \left(-2\lambda^2 + d - 1\right) = 0,
\] (A.10)

from which we read the eigenvalues of $F^{(1)}$,

\[
\lambda = \begin{cases}
\pm \sqrt{\frac{d - 1}{2}} & \text{multiplicity 1} \\
0 & \text{multiplicity } d - 2
\end{cases}
\] (A.11)

Next we calculate the eigenvalues of $F_1^{(1)} = F^{(1)} - \alpha G_{2,1}$. The matrix representation of $F_1^{(1)}$ is given by
\[
F_{1}^{(1)} = \begin{pmatrix}
0 & 1 - \alpha & 1 & \cdots & 1 \\
\frac{1 - \alpha}{\sqrt{2}} & 0 & \cdots & \cdots & 0 \\
\frac{1}{\sqrt{2}} & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\frac{1}{\sqrt{2}} & 0 & \cdots & \cdots & 0
\end{pmatrix}, \quad (A.12)
\]

and therefore the eigenvalue equation reads
\[
\begin{pmatrix}
-\lambda & 1 - \alpha & 1 & \cdots & 1 \\
\frac{1 - \alpha}{\sqrt{2}} & -\lambda & \cdots & \cdots & 0 \\
\frac{1}{\sqrt{2}} & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\frac{1}{\sqrt{2}} & 0 & \cdots & \cdots & -\lambda
\end{pmatrix} = 0.
\]

Using the identity of equation (A.8), with the matrices \(A, B, C,\) and \(D\) defined as before, we obtain the polynomial,
\[
\lambda^{d-2} \left( -2\lambda^2 + (1 - \alpha)^2 + d - 2 \right) = 0,
\]

from which we read the eigenvalues of \(F_{1}^{(1)},\)
\[
\lambda = \begin{cases}
\pm \sqrt{\frac{(1 - \alpha)^2 + d - 2}{2}} & \text{multiplicity 1} \\
0 & \text{multiplicity } d - 2
\end{cases} \quad (A.15)
\]

These eigenvalues are also the eigenvalues of \(F_{n}^{(1)}\) for \(n = 1, 2, \ldots, d\) since the matrix representation of \(F_{n}^{(1)}\) is the same as the matrix of \(F_{1}^{(1)}\) up to the location of \(1 - \alpha\) in the first row and column. Actually the eigenvalues of \(F^{(1)}\) and \(F_{1}^{(1)}\) are also the eigenvalues of \(F^{(b)}\) and \(F_{n}^{(b)}\) for all \(b = 1, 2, \ldots, d,\) and \(n = 1, 2, \ldots, d.\) This follows by transforming the matrix representation of \(F^{(b)}\) (or of \(F_{n}^{(b)}\)) to have a similar structure as the matrix of \(F^{(1)}\) \((F_{n}^{(1)})\), with an even number of rows and column permutation. Therefore, the eigenvalues equation, and therefore the eigenvalues, of the (permuted) \(F^{(b)}\) \((F_{n}^{(1)})\) are the same as the eigenvalues of \(F^{(1)}\) \((F_{n}^{(1)})\). Since \(\beta = \sqrt{\frac{d-1}{2}} = \sqrt{\frac{(1-\alpha)^2 + d - 2}{2}}\) we conclude that the eigenvalues of \(F_{n}^{(b)}\) of equation (5) are
\[
\left( \pm \beta \sqrt{\frac{d-1}{2}}, 0 \right) \quad \text{for } b = 1, 2, \ldots, d, \text{ and } n = 1, 2, \ldots, d, \text{ and therefore,}
\]

\[-\frac{1}{d} \sqrt{\frac{2}{d-1}} \leq t^{(b)} \leq \frac{1}{d} \sqrt{\frac{2}{d-1}} \text{ for } b = 1, 2, \ldots, d, \forall n. \quad (A.16)\]

We are now considering the last row of the correspondence of equation (A.4). Here the $F_n^{(b=d+1)}$ are all represented as diagonal matrices and therefore it is easy to read their eigenvalues. By noting that the maximal eigenvalue of $F_n^{(b)}$ equals $\sum_{n=1}^{d-1} \frac{1}{\sqrt{n(n+1)}}$, its minimal eigenvalue equals $-\sqrt{(d-1)/d}$, and inspecting the various other eigenvalues it is not difficult to show that
\[-\sqrt{\frac{d-1}{d}} - \frac{\alpha}{\sqrt{2}} \leq t^{(d+1)} \leq \sum_{n=1}^{d-1} \frac{1}{\sqrt{n(n+1)}} + \frac{\alpha}{\sqrt{2}}. \quad (A.17)\]

Following the discussion just below equation (11), we conclude that $t_{\text{opt}} = \frac{1}{d} \sqrt{\frac{2}{d-1}}$, and therefore $\kappa_{\text{opt}} = \frac{1}{d} + \frac{2}{d^2}$.

**Appendix B. A measurement with $d^2$ outcomes**

Let us consider the following measurement with $d^2$ outcomes, which is related to the MUM,
\[\Pi_n^{(b)} = \frac{1}{d + 1} P_n^{(b)}, \quad b = 1, 2, \ldots, d + 1, \quad n = 1, 2, \ldots, d - 1\]
\[\Pi_{d^2} = 1 - \sum_{b=1}^{d+1} \sum_{n=1}^{d-1} \Pi_n^{(b)} = \frac{1}{d + 1} \sum_{b=1}^{d+1} P_d^{(b)}. \quad (B.1)\]

We can regard this measurement as our MUM but with all of the last outcomes in each measurement, $P_d^{(b)}$ collected into one element $\Pi_{d^2}$. The probability of obtaining the outcome $\Pi_{d^2}$ is $\frac{1}{d + 1} \sum_{b=1}^{d+1} P_d^{(b)}$, where $P_d^{(b)}$ is the probability of obtaining the outcome $P_d^{(b)}$. This implies that we can rewrite equation (12) as
\[\rho = (d + 1) \left( \sum_{b=1}^{d+1} \sum_{n=1}^{d-1} \frac{P_n^{(b)} R_n^{(b)}}{d + 1} + \sum_{b=1}^{d+1} \frac{P_d^{(b)} R_d^{(b)}}{d + 1} \right), \quad (B.2)\]
from which we read the reconstruction operators of the $\Pi$
\[\Theta_n^{(b)} = (d + 1) R_n^{(b)}, \quad b = 1, 2, \ldots, d + 1, \quad n = 1, 2, \ldots, d - 1,\]
\[\Theta_{d^2} = (d + 1) \sum_{b=1}^{d+1} R_d^{(b)}. \quad (B.3)\]

**Appendix C. Proof of Theorem 2**

**Proof.** We first note that the $P_n^{(b)}$s, upon subtracting the completely mixed states, $P_n^{(b)} - \frac{1}{d} = F_n^{(b)}$, define $d + 1$ orthogonal subspaces of operators acting on a $d$-dimensional Hilbert space. Therefore, any quantum state can be written as
\[ \rho = \frac{1}{d} + \sum_{n=1}^{d+1} \sum_{b=1}^{d} r_n^{(b)} F_n^{(b)}. \]  \hspace{1cm} (C.1)

In particular, for pure states \( \text{Tr} (\rho^2) = 1 \), which together with the first identity of equation (6) imply
\[ \sum_{b=1}^{d+1} \left[ d \sum_{n=1}^{d} \left( r_n^{(b)} \right)^2 - \left( \sum_{n=1}^{d} r_n^{(b)} \right)^2 \right] = \frac{d - 1}{d(1 + \sqrt{d})^2}, \]  \hspace{1cm} (C.2)

Next, consider the MUM \( \mathcal{P}^{(b)} \) of equation (8). The probability distribution of \( \mathcal{P}^{(b)} \) given a state \( \rho \) is
\[ p_n^{(b)} = \text{Tr} \left( p_n^{(b)} \rho \right) = \frac{1}{d} + t \left( 1 + \sqrt{d} \right)^2 \left( d r_n^{(b)} - \sum_{n=1}^{d} r_n^{(b)} \right), \]  \hspace{1cm} (C.3)

To prove the theorem we use the inequality [24, 25],
\[ H (\mathcal{P}^{(b)}, \rho) = - \sum_{n=1}^{d} p_n^{(b)} \log p_n^{(b)} \geqslant -\log \sum_{n=1}^{d} \left( p_n^{(b)} \right)^2, \]  \hspace{1cm} (C.4)

which holds for any probability distribution. Summing over \( d + 1 \) MUM and dividing by \( d + 1 \), we obtain,
\[ \frac{d+1}{d+1} \sum_{b=1}^{d+1} H (\mathcal{P}^{(b)}, \rho) \geqslant - \frac{1}{d + 1} \sum_{b=1}^{d+1} \log \sum_{n=1}^{d} \left( p_n^{(b)} \right)^2 \geqslant -\log \frac{1}{d + 1} \sum_{b=1}^{d+1} \sum_{n=1}^{d} \left( p_n^{(b)} \right)^2, \]  \hspace{1cm} (C.5)

where the second inequality is a consequence of the concavity of the log function. By using equations (6), (C.2), and (C.3), one can show that for pure states
\[ \sum_{b=1}^{d+1} \sum_{n=1}^{d} \left( p_n^{(b)} \right)^2 = \frac{1}{d} \left( d + 1 \right) + t^2 \left( 1 + \sqrt{d} \right)^2 (d - 1) = 1 + \kappa. \]  \hspace{1cm} (C.6)

Plugging this into equation (C.5) we arrive at equation (16). \( \square \)

References

[1] Englert B-G 2006 Lectures on Quantum Mechanics-Perturbed Evolution (Singapore: World Scientific)
[2] Ivanovic I D 1981 J. Phys. A: Math. Gen. 14 3241
[3] Englert B-G and Aharonov Y 2001 Phys. Lett. A 284 1
[4] Aravind P K 2003 Z. Naturforsch. 58a 85
[5] Wootters W K 2006 Found. Phys. 36 112
[6] Klappenecker A and Rötteler M 2005 Proc. Int. Symp. Inf. Theory pp 1740–4
[7] Gross D, Audenaert K and Eisert J 2007 J. Math. Phys. 48 052104
[8] Spengler C and Kraus B 2013 Phys. Rev. A 88 052323
[9] Gottesman D 1996 Phys. Rev. A 54 1862
[10] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1997 Phys. Rev. Lett. 78 405
[11] Bruß D and Macchiavello C 2002 Phys. Rev. Lett. 88 127901
[12] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 Phys. Rev. Lett. 88 127902
[13] Adamson R B A and Steinberg A M 2010 Phys. Rev. Lett. 105 030406
[14] Wootters W K and Fields B D 1989 Ann. Phys. (NY) 191 363
[15] Spengler C, Huber M, Brierley S, Adaktylos T and Hiesmayr B C 2012 Phys. Rev. A 86 022311
[16] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 Algorithmica 34 512
[17] Klappenecker A and Rötteler M 2004 Lect. Notes Comp. Science 2948 262
[18] Durt T 2005 J. Phys. A: Math. Gen. 38 5267
[19] Durt T, Englert B-G, Bengtsson I and Życzkowski K 2010 Int. J. Quant. Inf. 8 535
[20] Grassl M 2009 arXiv:quant-ph/0406175
[21] Brierley S and Weigert S 2008 Phys. Rev. A 78 042312
[22] Brierley S and Weigert S 2010 J. Phys.: Conf. Ser. 254 012008
[23] Raynal P, Lu X and Englert B-G 2011 Phys. Rev. A 83 062303
[24] Ivanovic I D 1992 J. Phys.: Math. Gen. 25 363
[25] Wehner S and Winter A 2010 New J. Phys. 12 025009
[26] Friedland S, Gheorghiu V and Gour G 2013 Phys. Rev. Lett. 111 230401