On Estimating the State of a Finite Level Quantum System
by
K. R. Parthasarathy
Indian Statistical Institute, Delhi Centre,
7, S. J. S. Sansanwal Marg,
New Delhi - 110 016, India.
e-mail : krp@isid.ac.in

Summary : We revisit the problem of mutually unbiased measurements in the context of estimating the unknown state of a $d$-level quantum system, first studied by W. K. Wootters and B. D. fields[7] in 1989 and later investigated by S. Bandyopadhyay et al [3] in 2001 and A. O. Pittenger and M. H. Rubin [6] in 2003. Our approach is based directly on the Weyl operators in the $L^2$-space over a finite field when $d = p^r$ is the power of a prime. When $d$ is not a prime power we sacrifice a bit of optimality and construct a recovery operator for reconstructing the unknown state from the probabilities of elementary events in different measurements.

Key words : Mutually unbiased measurements, finite field, Weyl operators, error basis.

AMS 2000 Mathematics Subject Classification 47L90, 47N50, 81P68 (?)

1 Introduction

This is almost an expository account of a well-known problem of quantum probability and statistics arising in the context of quantum information theory. There is a $d$-level quantum system whose pure states are described by unit vectors in a $d$-dimensional complex Hilbert space $\mathcal{H}$ equipped with the scalar product $\langle \varphi | \psi \rangle$ between elements $\varphi, \psi$
in $\mathcal{H}$. This scalar product is linear in the variable $\psi$ and antilinear in the variable $\varphi$.

Throughout this exposition we assume that $d$ is finite. Denote by $\mathcal{B}(\mathcal{H})$ the $\ast$-algebra of all operators on $\mathcal{H}$. The complex $d^2$-dimensional vector space $\mathcal{B}(\mathcal{H})$ will also be viewed as a Hilbert space with the scalar product $\langle X|Y \rangle = \text{Tr} X^\dagger Y$ where $X^\dagger$ denotes the adjoint of the operator $X$. Denote by $\mathcal{S}(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ the compact convex set of all nonnegative (definite) operators of unit trace. Any element $\rho$ in $\mathcal{S}(\mathcal{H})$ is called a state of the system. The extreme points of $\mathcal{S}(\mathcal{H})$ are precisely one dimensional orthogonal projections. They are called pure states. In the Dirac notation any pure state can be expressed as $|\psi \rangle\langle \psi|$ where $\psi$ is a unit vector in $\mathcal{H}$.

Denote by $\mathcal{P}(\mathcal{H})$ the set of all orthogonal projection operators (or, simply, projections) on $\mathcal{H}$. Any element $P$ in $\mathcal{P}(\mathcal{H})$ is called an event concerning the system and the quantity $\text{Tr} \rho P$ is interpreted as the probability of the event $P$ in the state $\rho$. In the context of quantum information theory the state of a quantum system can be utilized as an information resource. If the system is in an unknown state $\rho$ it is important to estimate $\rho$ from “independent repeated measurements”. If we choose and fix an orthonormal basis $\{e_0, e_1, \ldots, e_{d-1}\}$ in $\mathcal{H}$ then $\rho$ is described in this basis by a nonnegative definite matrix $((\rho_{ij}))$ where $\rho_{ij} = \langle e_i|\rho|e_j \rangle$.

Thus determination of $\rho$ involves the determination of $d^2-1$ real parameters, namely, $\rho_{ii}, i = 1, 2, \ldots, d-1$, $\text{Re} \rho_{ij}, \text{Im} \rho_{ij}, 0 \leq i < j \leq d-1$. (Note that $\rho_{00} = 1 - \sum_{i=1}^{d-1} \rho_{ii}$ and $\rho_{ij} = \bar{\rho}_{ji}$.)

By an elementary measurement $\mathcal{M} = \{P_0, P_1, \ldots, P_{d-1}\}$ we mean a family of $d$ mutually orthogonal one dimensional projection operators $P_j, j = 0, 1, 2, \ldots, d-1$ so that $\sum_0^{d-1} P_j = I$, the identity operator. If the measurement $\mathcal{M}$ is performed when the state of the system is $\rho$, the result of such a measurement is one of the classical outcomes $j \in \{0, 1, 2, \ldots, d-1\}$ with probability $\text{Tr} \rho P_j = p_j$ for each $j$. Independent repeated trials of the measurement in the same state $\rho$ yield frequencies $f_j$ for each elementary outcome $j$ and $f_j$ can be viewed as an estimate of $p_j$ for each $j$. Thus an elementary measurement covers at most $d-1$ degrees of freedom concerning $\rho$ in view of the relation $\sum_0^{d-1} p_j = 1$. In order to estimate $\rho$ it is therefore necessary to examine the frequencies of elementary outcomes in at least $d+1$ elementary measurements $\mathcal{M}_j, 0 \leq j \leq d$ where no two of the measurements $\mathcal{M}_i$ and $\mathcal{M}_j$ have any “overlap of information”. Such an attempt is likely to cover all $(d+1)(d-1) = d^2-1$ degrees of freedom involved in recon-
structing or estimating the unknown \( \rho \). To bring clarity to the notion of “nonoverlap of information” in a pair of elementary measurements it is useful to look at the \( \star \)-abelian algebra

\[
\mathcal{A}(\mathcal{M}) = \left\{ \sum_{j=0}^{d-1} a_j P_j \mid a_j \in \mathbb{C}, j = 0, 1, \ldots, d - 1 \right\}.
\]

Any element \( X = \sum_{j=0}^{d-1} x_j P_j \) in \( \mathcal{A}(\mathcal{M}) \) can be looked upon as a complex-valued observable where \( P_j \) is interpreted as the event that “\( X \) assumes the value \( x_j \)”. Of course, this is justified if all the \( x_j \)'s are distinct scalars. If \( x \) is any scalar then the event that \( X \) assumes the value \( x \) is the projection \( \sum_{j : x_j = x} P_j \). Thus the subalgebra \( \mathbb{C}I \subset \mathcal{A}(\mathcal{M}) \) consists precisely of constant-valued observables. Such an interpretation motivates the following formal definition.

**Definition 1.1** Two elementary measurements \( \mathcal{M} = \{P_0, P_1, \ldots, P_{d-1}\} \), \( \mathcal{M}' = \{Q_0, Q_1, \ldots, Q_{d-1}\} \) are said to be weakly mutually unbiased (WMUB) if

\[ \mathcal{A}(\mathcal{M}) \cap \mathcal{A}(\mathcal{M}') = \mathbb{C}I, \]

and strongly mutually unbiased (SMUB) if, in the Hilbert space \( \mathcal{B}(\mathcal{H}) \), the subspaces \( \mathcal{A}(\mathcal{M}) \oplus \mathbb{C}I \) and \( \mathcal{A}(\mathcal{M}') \oplus \mathbb{C}I \) are mutually orthogonal. (Here, for two subspaces \( S_1 \subset S_2 \subset \mathcal{B}(\mathcal{H}) \), \( S_2 \ominus S_1 \) denotes the orthogonal complement of \( S_1 \) in \( S_2 \)).

Clearly SMUB implies WMUB. We shall now describe these two properties in terms of the quantities \( \text{Tr} P_i Q_j \).

**Proposition 1.2** Two elementary measurements \( \mathcal{M} = \{P_0, P_1, \ldots, P_{d-1}\} \), \( \mathcal{M}' = \{Q_0, Q_1, \ldots, Q_{d-1}\} \) are SMUB if and only if

\[ \text{Tr} P_i Q_j = d^{-1} \quad \text{for all } i, j, \in \{0, 1, 2, \ldots, d - 1\}. \quad (1.1) \]

**Proof:** Note that the subspaces \( \mathcal{A}(\mathcal{M}) \oplus \mathbb{C}I \) and \( \mathcal{A}(\mathcal{M}') \oplus \mathbb{C}I \) are respectively spanned by the subsets \( \{P_j - d^{-1}I, 0 \leq j \leq d - 1\} \) and \( \{Q_j - d^{-1}I, 0 \leq j \leq d - 1\} \). Thus the orthogonality of these two subspaces is equivalent to the condition

\[ 0 = \langle P_i - d^{-1}I \mid Q_j - d^{-1}I \rangle = \text{Tr}(P_i - d^{-1}I)(Q_j - d^{-1}I) = (\text{Tr} P_i Q_j) - d^{-1} \]

\[ = \text{Tr} P_i Q_j - d^{-1} \]

Thus, for SMUB, \( \text{Tr} P_i Q_j = d^{-1} \). Conversely, if \( \text{Tr} P_i Q_j = d^{-1} \) then \( \mathcal{A}(\mathcal{M}) \cap \mathcal{A}(\mathcal{M}') = \mathbb{C}I \), and by the span conditions, SMUB follows.
for all $i, j$ in $\{0, 1, 2, \ldots, d - 1\}$. □

**Proposition 1.3** Let $\mathcal{M} = \{P_0, P_1, \ldots, P_{d-1}\}$, $\mathcal{M}' = \{Q_0, Q_1, \ldots, Q_{d-1}\}$ be two elementary measurements. Suppose

$$L = [\text{Tr}(P_i - P_0)(Q_j - Q_0)], \ i, j \in \{1, 2, \ldots, d - 1\}$$

and $J_{d-1}$ is the $(d - 1) \times (d - 1)$ matrix all the entries of which are unity. Then $\mathcal{M}$ and $\mathcal{M}'$ are WMUB if and only if

$$\det \left( I_{d-1} + J_{d-1} + d^{-1}LJ_{d-1}L^\dagger - LL^\dagger \right) > 0. \quad (1.2)$$

**Proof:** Let $X \in \mathcal{A}(\mathcal{M}) \cap \mathcal{A}(\mathcal{M}')$. Then there exist scalars $a_i, b_j, i, j \in \{1, 2, \ldots, d - 1\}$ such that

$$X = d^{-1}(\text{Tr}X)I + \sum_{i=1}^{d-1} a_i (P_i - P_0)$$

$$= d^{-1}(\text{Tr}X)I + \sum_{j=1}^{d-1} b_j (Q_j - Q_0).$$

Thus $\mathcal{M}$ and $\mathcal{M}'$ are WMUB if and only if the set $\{P_1 - P_0, P_2 - P_0, \ldots, P_{d-1} - P_0, Q_1 - Q_0, Q_2 - Q_0, \ldots, Q_{d-1} - Q_0\}$ of $2(d - 1)$ elements in the Hilbert space $\mathcal{B}(\mathcal{H})$ is linearly independent. This, in turn, is equivalent to the strict positive definiteness of the partitioned matrix

$$
\begin{bmatrix}
[\text{Tr}(P_i - P_0)(P_j - P_0)] & [\text{Tr}(P_i - P_0)(Q_j - Q_0)] \\
[\text{Tr}(Q_i - Q_0)(P_j - P_0)] & [\text{Tr}(Q_i - Q_0)(Q_j - Q_0)]
\end{bmatrix}, \ i, j \in \{1, 2, \ldots, d - 1\}
$$

of order $2(d - 1)$. We have

$$\text{Tr}(P_i - P_0)(P_j - P_0) = \text{Tr}(Q_i - Q_0)(Q_j - Q_0) = \begin{cases} 2 & \text{if } i = j, \\ 1 & \text{if } i \neq j. \end{cases}$$

Thus, $\mathcal{M}$ and $\mathcal{M}'$ are WMUB if and only if

$$\begin{bmatrix}
I_{d-1} + J_{d-1} & L \\
L^\dagger & I_{d-1} + J_{d-1}
\end{bmatrix}$$
has a strictly positive determinant. Left multiplication of this matrix by the matrix

\[
\begin{bmatrix}
I_{d-1} & -L(I_{d-1} + J_{d-1})^{-1} \\
0 & I_{d-1}
\end{bmatrix}
\]

with unit determinant yields the equivalent condition

\[
\det \left( I_{d-1} + J_{d-1} - L(I_{d-1} + J_{d-1})^{-1}L^\dagger \right) > 0.
\]  \hspace{1cm} (1.3)

Since

\[
(I_{d-1} + J_{d-1})^{-1} = I_{d-1} - d^{-1}J_{d-1},
\]

condition (1.3) reduces to condition (1.2). \square

**Corollary 1.4** If the matrix $L$ of Proposition 1.3 satisfies the inequality $\|L\| < 1$ (where $\|\cdot\|$ is the standard operator norm in the $\star$-algebra $\mathcal{B}(\mathbb{C}^{d-1})$) then $\mathcal{M}$, $\mathcal{M}'$ are WMUB. Furthermore $\mathcal{M}$, $\mathcal{M}'$ are SMUB if and only if $L = 0$.

**Proof:** Immediate. \square

In the context of minimizing the number of elementary measurements required for estimating the state $\rho$ of a quantum system Proposition 1.2 emphasizes the importance of the search for $d + 1$ elementary measurements which are pairwise SMUB. When $d$ is a prime power $p^r$ the existence of such a family of SMUB measurements was proved by Wootters and Fields [7]. Alternative proofs of this result were given by S. Bandyopadhyay et al in [3] and Pittenger and Rubin in [6]. In this paper we shall present a proof of the same result by using the commutation relations of Weyl operators in the $L^2$ space of the finite field $\mathbb{F}_{p^r}$. When $d = p_1^{m_1}p_2^{m_2} \ldots p_n^{m_n}$ with $p_i$’s being prime we shall use the Weyl commutation relations in the $L^2$ space of the additive abelian group $\otimes_{i=1}^n \mathbb{F}_{p_i^{m_i}}$ and study the problem of estimating the unknown state of a $d$-level system. This leads to an interesting reconstruction formula for a state $\rho$ in terms of probabilities of $d^2 - 1$ events arising from $\prod_{i=1}^n (p_i^{m_i} + 1)$ elementary measurements. However, one would like to express $\rho$ in terms of the probabilities of elementary outcomes in $(\prod_{i=1}^n p_i^{m_i} + 1)$ elementary measurements.
2 The case \( d = p^r \)

Let \( \dim \mathcal{H} = d = p^r \) be a prime power. For any prime power \( q \) denote by \( \mathbb{F}_q \) the unique (upto a field isomorphism) finite field of cardinality \( q \). Choose and fix any nontrivial character \( \chi \) of the additive group \( \mathbb{F}_d \) and put

\[
\langle x, y \rangle = \chi(xy), \ x, y \in \mathbb{F}_d. \tag{2.1}
\]

One can, for example, look upon \( \mathbb{F}_d \) as an \( r \)-dimensional vector space over \( \mathbb{F}_p \), express any element \( x \) in \( \mathbb{F}_d \) as an ordered \( r \)-tuple: \( x = (s_1, s_2, \ldots, s_r) \) where \( 0 \leq s_i \leq p - 1 \) for each \( i \) and put

\[
\chi(x) = \exp \frac{2\pi i}{p}s_1. \tag{2.2}
\]

Then we have \( |\langle x, y \rangle| = 1 \), \( \langle x, y \rangle = \langle y, x \rangle \), \( \langle x, y_1 + y_2 \rangle = \langle x, y_1 \rangle \langle x, y_2 \rangle \) and \( x = 0 \) if \( \langle x, y \rangle = 1 \) for all \( y \) in \( \mathbb{F}_d \). In other words, \( \langle ., . \rangle \) is a nondegenerate symmetric bicharacter for \( \mathbb{F}_d \). Identify the Hilbert space \( \mathcal{H} \) with \( L^2(\mathbb{F}_d) \), using the counting measure in \( \mathbb{F}_d \), and put

\[
| x > = 1_{\{x\}}, x \in \mathbb{F}_d
\]

where \( 1_{\{x\}} \) is the indicator function of the singleton subset \( \{x\} \) in \( \mathbb{F}_d \). Then \( \{ | x >, x \in \mathbb{F}_d \} \) is an orthonormal basis for \( \mathcal{H} \) labelled by the elements of \( \mathbb{F}_d \). Now, consider the unique unitary operators \( U_a, U_b \) in \( \mathcal{H} \) determined by the relations

\[
U_a|x > = |a + x >,
V_b|x > = < b, x | x > \quad \text{for all } x \in \mathbb{F}_d.
\]

Then we have

\[
U_aU_b = U_{a+b}, V_aV_b = V_{a+b}, \tag{2.3}
\]

\[
V_bU_a = \langle a, b \rangle U_aV_b. \tag{2.4}
\]

Elementary algebra shows that

\[
\text{Tr} \ (U_{a_1}V_{b_1})^\dagger U_{a_2}V_{b_2} = d\delta_{a_1,a_2}\delta_{b_1,b_2} \tag{2.5}
\]

for all \( a_1, a_2, b_1, b_2 \) in \( \mathbb{F}_d \). In particular, the family \( \{U_aV_b, a, b \in \mathbb{F}_d\} \) of \( d^2 \) unitary operators constitute an orthogonal basis for the Hilbert space \( \mathcal{B}(\mathcal{H}) \). This is an example of a unitary
error basis in the theory of error correcting quantum codes [4]. Notice also the fact that \( \{U_a\} \) and \( \{V_b\} \) are like the position and momentum representations obeying the Weyl commutation relations in classical quantum mechanics. In view of this property we call any operator of the form \( \lambda U_aV_b, |\lambda| = 1, a, b \in \mathbb{F}_d \) a Weyl operator. We say that (2.3) and (2.4) constitute the Weyl commutation relations. The usefulness of such an error basis of Weyl operators in the study of quantum codes has been explored in [1], [2], [5].

We shall slightly modify the error basis \( \{U_aV_b\} \) by multiplying each element \( U_aV_b \) by an appropriate phase factor. Once again viewing \( \mathbb{F}_d \) as an \( r \)-dimensional vector space over \( \mathbb{F}_p \), expressing any \( x \in \mathbb{F}_d \) as an ordered \( r \)-tuple \( x = (s_1, s_2, \ldots, s_r) \) with \( 0 \leq s_i \leq p - 1 \) for each \( i \) and considering the basis elements \( e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \) of the field \( \mathbb{F}_d \) with 1 in the \( i \)-th position and 0 elsewhere we write \( x = s_1e_1 + s_2e_2 + \cdots + s_re_r \) and define

\[
\alpha(a, x) = \chi\left(a \left\{ \sum_{i<j} s_is_j e_i e_j + \sum_j s_j(s_j - 1) e_j^2 \right\} \right), a, x \in \mathbb{F}_d
\]

where \( \chi \) is the character chosen and fixed at the beginning of this section.

Now put \( \overline{\mathbb{F}}_d = \mathbb{F}_d \cup \{\infty\} \) and write

\[
W(a, x) = \begin{cases} 
\alpha(a, x)U_xV_{ax} & \text{if } a \in \mathbb{F}_d, x \in \mathbb{F}_d, \\
V_x & \text{if } a = \infty.
\end{cases}
\]

Then we have the following proposition.

**Proposition 2.1** The family \( \{I, W(a, x), a \in \overline{\mathbb{F}}_d, x \in \mathbb{F}_d \} \) is an orthogonal basis of unitary operators for the operator Hilbert space \( B(\mathcal{H}) \) satisfying the relations

\[
W(a, x)W(a, y) = W(a, x + y) \text{ for all } a \in \overline{\mathbb{F}}_d, x \in \mathbb{F}_d.
\]

**Proof:** The first part is immediate from the fact that the family of operators under consideration differs from the family \( \{U_xV_y, x, y \in \mathbb{F}_d\} \) only by a scalar factor of modulus unity in each element. If \( a \in \mathbb{F}_d, x = \sum s_i e_i, y = \sum t_i e_i \) we have from (2.3) (2.4)

\[
W(a, x)W(a, y) = \alpha(a, x)\alpha(a, y)(ax, y)U_{x+y}V_{a(x+y)} = \alpha(a, x)\alpha(a, y)\alpha(a, x+y)(ax, y)W(a, x+y)
\]
where the coefficient of $W(a, x + y)$ is of the form $\chi(az)$ with
\[
  z = \sum_{i < j} s_i s_j e_i e_j + \sum_j s_j^2 e_j^2 + \sum_{i < j} t_i t_j e_i e_j + \sum_j t_j(t_j - 1) e_j^2
  - \sum_{i < j} (s_i + t_i)(s_j + t_j) e_i e_j - \sum_j (s_j + t_j)(s_j + t_j - 1) e_j^2
  + \sum_{i,j} s_i t_j e_i e_j
\]
\[
  = 0.
\]
This proves (2.8) when $a \in \mathbb{F}_d$. When $a = \infty$, (2.8) is a part of (2.3). $\blacksquare$

**Theorem 2.2** There exists a family of one dimensional orthogonal projection operators
\{ $P(a, x), a \in \mathbb{F}_d, x \in \mathbb{F}_d$ \} satisfying the following:

(i) $W(a, x) = \sum_{y \in \mathbb{F}_d} \langle x, y \rangle P(a, y)$

(ii) $P(a, y) = d^{-1} \sum_{x \in \mathbb{F}_d} \overline{\langle x, y \rangle} W(a, x)$,

(iii) $P(a, x)P(a, y) = \delta_{x,y} P(a, x)$,

(iv) $\sum_{x \in \mathbb{F}_d} P(a, x) = I$,

(v) $\text{Tr} P(a, x)P(b, y) = d^{-1}$ for all $a \neq b; a, b \in \mathbb{F}_d; x, y \in \mathbb{F}_d$.

**Proof:** By Proposition 2.1 the correspondence $x \rightarrow W(a, x)$ is a unitary representation of the additive abelian group $\mathbb{F}_d$ and \{ $(\cdot, y), y \in \mathbb{F}_d$ \} is the set of all its characters. Thus the decomposition of $\{W(a, \cdot)\}$ into its irreducible components yields a spectral measure $P(a, \cdot)$ on $\mathbb{F}_d$ satisfying (i), (iii) and (iv). Substituting from (i) the expression for $W(a, x)$ in the right hand side of (ii) and using the orthogonality relations for characters we get (ii). Taking trace on both the sides of (ii) and observing that $W(a, 0) = I$ and $\text{Tr} W(a, x) = 0$ for $x \neq 0$ we get $\text{Tr} P(a, y) = 1$. Thus each $P(a, y)$ is a one dimensional projection. Substituting for $P(a, x)$ and $P(a, y)$ from (ii) in the left hand side of (v) we have from (2.7), (2.3) and (2.4)
\[
  \text{Tr} P(a, x)P(b, y)
  = d^{-2} \sum_{z_1, z_2 \in \mathbb{F}_d} \langle x, z_1 \rangle \langle y, z_2 \rangle \text{Tr} W(a, z_1)W(b, z_2)
  = d^{-2} \sum_{z_1, z_2 \in \mathbb{F}_d} \langle x, z_1 \rangle \langle y, z_2 \rangle \alpha(a, z_1)\alpha(b, z_2)\langle az_1, z_2 \rangle \text{Tr} U_{z_1+bz_2} V_{az_1+bz_2}.
\]
Now observe that the \((z_1, z_2)\)-th term of the sum on the right hand side is nonzero only if \(z_1 + z_2 = 0\), \(a z_1 + b z_2 = 0\). If \(a \neq b\) this is possible only if \(z_1 = z_2 = 0\). This proves (v).

\[\Box\]

**Corollary 2.3** Let \(\mathcal{M}_a = \{P(a, x), x \in \mathbb{F}_d\}\). Then \(\{\mathcal{M}_a, a \in \mathbb{F}_d\}\) is a set of \((d + 1)\) elementary measurements which are pairwise SMUB.

**Proof:** Immediate from Proposition 1.2. \(\Box\)

Our next result yields a recovery formula for any state \(\rho\) from the probability distributions \(\{\text{Tr} \, \rho P(a, x), x \in \mathbb{F}_d\}\) on \(\mathbb{F}_d\) arising from the measurements \(\{\mathcal{M}_a, a \in \mathbb{F}_d\}\).

**Theorem 2.4** Let \(\{P(a, x), a \in \mathbb{F}_d, x \in \mathbb{F}_d\}\) be the projections in Theorem 2.2. Then, for any state \(\rho\) on \(L^2(\mathbb{F}_d)\) the following holds:

\[(\text{i}) \quad \rho = \sum_{a \in \mathbb{F}_d} \sum_{z \in \mathbb{F}_d} \left\{ \text{Tr} \, \rho P(a, z) - \frac{1}{d+1} \right\} P(a, z)\]

\[(\text{ii}) \quad \rho = \sum_{x, y \in \mathbb{F}_d} \sum_{a \in \mathbb{F}_d} \overline{\langle x, y \rangle} \{\text{Tr} \, \rho P(a, y)\} W(a, x)\]

**Proof:** From the first part of Proposition 2.1, it follows that \(\rho\) admits the expansion

\[\rho = d^{-1} \left\{ I + \sum_{a \in \mathbb{F}_d \backslash \{0\}} \left[ \text{Tr} \, \rho W(a, x)^\dagger \right] W(a, x) \right\}\]

in terms of the orthogonal basis arising from the Weyl operators. Now substitute in the right hand side the expressions for \(W(a, x)\) in (i) of Theorem 2.2 and use the orthogonality relations for characters:

\[\sum_{x \in \mathbb{F}_d} \overline{\langle x, y \rangle} \langle x, z \rangle = d \delta_{y,z}\]

Then we obtain the identity (i) of the theorem. If we substitute for \(P(a, z)\) from the identity (ii) of Theorem 2.2 we obtain the second identity of the theorem. \(\Box\)

**Remark:** If we make repeated independent measurements \(\mathcal{M}_a\), obtain the frequencies for the different events \(P(a, z)\) and substitute those frequencies for the different probabilities \(\text{Tr} \, \rho P(a, z)\) in the unknown state \(\rho\) we will get an unbiased and asymptotically consistent
estimate $\tilde{\rho}$ of $\rho$ but $\tilde{\rho}$ may not be a positive operator. One may replace $\tilde{\rho}$ by the normalised version of the positive part or the modulus of $\tilde{\rho}$ at the cost of losing unbiasedness. This also increases the computational cost.

### 3 Estimation of states in the general case

Let $d = p_1^{m_1}p_2^{m_2}\ldots p_n^{m_n}$ be the decomposition of $d$ into its prime factors $p_1 < p_2 < \cdots < p_n$. Write $d_j = p_j^{m_j}$. We may identify the $d$-dimensional Hilbert space $\mathcal{H}$ with $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ where $\mathcal{H}_j = L^2(\mathbb{F}_{d_j})$, $\mathbb{F}_{d_j}$ being the finite field of cardinality $d_j$.

Following the definition in (2.7) construct the unitary operators $W^{(j)}(a_j, x_j)$ when $d = d_j$, $j = 1, 2, \ldots, n$ and using Theorem 2.2, the corresponding projections $P^{(j)}(a_j, x_j)$, where $a_j \in \mathbb{F}_{d_j}$, $x_j \in \mathbb{F}_{d_j}$. We now adopt the following convention: for any operator $X$ in $L^2(\mathbb{F}_{d_j}) = \mathcal{H}_j$ denote by the same symbol $X$ the operator in $\mathcal{H}$ defined by $X = X_1 \otimes X_2 \otimes \cdots \otimes X_n$ where $X_i$ is the identity operator in $\mathcal{H}_i$ when $i \neq j$ and $X_j = X$. The operator $X$ thus defined in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ is called the ampliation of $X$ in $\mathcal{H}_j$ to $\mathcal{H}$. Since $\mathcal{B}(\mathcal{H})$ can be identified with $\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2) \otimes \cdots \otimes \mathcal{B}(\mathcal{H}_n)$ as Hilbert spaces as well as $\mathcal{A}$-algebras it follows from Proposition 2.1 that the family

$$\mathcal{F} = \{ I, W^{(i_1)}(a_{i_1}, x_{i_1})W^{(i_2)}(a_{i_2}, x_{i_2}) \cdots W^{(i_\nu)}(a_{i_\nu}, x_{i_\nu}), \quad a_{i_j} \in \mathbb{F}_{d_j}, x_{i_j} \in \mathbb{F}_{d_j} \setminus \{0\}, j = 1, 2, \ldots, \nu, \quad 1 \leq i_1 < i_2 < \cdots < i_\nu \leq n, r = 1, 2, \ldots, n \} \quad (3.1)$$

of unitary operators in $\mathcal{H}$ constitute an orthogonal basis for the operator Hilbert spaces $\mathcal{B}(\mathcal{H})$. Note that the cardinality of $\mathcal{F}$ is, indeed, equal to

$$1 + \sum_{r=1}^{n} \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} (d_{i_1}^2 - 1)(d_{i_2}^2 - 1)\ldots(d_{i_r}^2 - 1)$$

$$= (1 + d_1^2 - 1)(1 + d_2^2 - 1)\ldots(1 + d_n^2 - 1)$$

$$= d_1^2 d_2^2 \ldots d_n^2$$

$$= d^2.$$
the dimension of $\mathcal{B}(\mathcal{H})$. For any subset $J = \{i_1, i_2, \ldots, i_r\} \subset \{1, 2, \ldots, n\}$ where $1 \leq i_1 < i_2 < \cdots < i_r \leq n$, define

$$d(J) = d_{i_1}d_{i_2} \cdots d_{i_r}$$

$$d'(J) = (d_{i_1} + 1)(d_{i_2} + 1) \cdots (d_{i_r} + 1),$$

and for any state $\rho$ in $\mathcal{H}$, put

$$S_\rho(J) = \sum_{a_{i_1}, y_{i_1} \in \mathbb{F}_{d_{i_1}}; a_{i_j}, y_{i_j} \in \mathbb{F}_{d_{i_j}}} \{\text{Tr} \rho P^{(i_1)}(a_{i_1}, y_{i_1})P^{(i_2)}(a_{i_2}, y_{i_2}) \cdots P^{(i_r)}(a_{i_r}, y_{i_r})\}$$

where $\{P^{(i)}(a_i, y_i)\}$ are the one dimensional projections in $\mathcal{H}_i$ determined by the unitary representation $x_i \rightarrow W^{(i)}(a_i, x_i)$ of the additive group $\mathbb{F}_{d_i}$ according to Theorem 2.2 and amplified to the product Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$. Thus $S_\rho(J)$ is an operator in $\mathcal{H}$ determined by the probabilities $\text{Tr} \rho P^{(i_1)}(a_{i_1}, y_{i_1})P^{(i_2)}(a_{i_2}, y_{i_2}) \cdots P^{(i_r)}(a_{i_r}, y_{i_r})$ and the projections $P^{(i_1)}(a_{i_1}, y_{i_1})P^{(i_2)}(a_{i_2}, y_{i_2}) \cdots P^{(i_r)}(a_{i_r}, y_{i_r})$ of dimension $\Pi_{j \notin \{i_1, i_2, \ldots, i_r\}} d_j$ with $a_i$'s varying in $\mathbb{F}_{d_i}$ and $y_i$'s in $\mathbb{F}_{d_i}$ for any $i$. With these notations and the convention $S_\rho(\emptyset) = I$, we have the following theorem for the recovery of $\rho$ from the probabilities.

**Theorem 3.1** Let $\rho$ be any state in $\mathcal{H}$. Then

$$\rho = \sum_{J \subseteq \{1, 2, \ldots, n\}} (-1)^{n-|J|} S_\rho(J)$$

(3.3)

where $S_\rho(J)$ is given by (3.2) and $|J|$ is the cardinality of $J$.

**Proof:** Since the family $\mathcal{F}$ of unitary operators in (3.1) is an orthogonal basis for $\mathcal{B}(\mathcal{H})$ we can expand the state $\rho$ in this basis as

$$\rho = (d_1d_2 \cdots d_n)^{-1} \left\{ I + \sum_{r=1}^{n} \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} \sum_{a_{i_j}, y_{i_j} \in \mathbb{F}_{d_{i_j}}; x_{i_j} \in \mathbb{F}_{d_{i_j}}} \left[ \text{Tr} \rho W^{(i_1)}(a_{i_1}, x_{i_1}) \cdots W^{(i_r)}(a_{i_r}, x_{i_r}) \right] W^{(i_1)}(a_{i_1}, x_{i_1}) \cdots W^{(i_r)}(a_{i_r}, x_{i_r}) \right\}.$$
From Theorem 2.2 we have for any fixed $i$

$$\sum_{x_i \in F_{d_i} \setminus \{0\}} W^{(i)}(a_i, x_i) \uparrow \otimes W^{(i)}(a_i, x_i)$$

$$= \sum_{y, z \in F_{d_i}} \overline{\langle x_i, y \rangle \langle x_i, z \rangle} P^{(i)}(a_i, y) \otimes P^{(i)}(a_i, z)$$

$$= d_i \sum_{y \in F_{d_i}} P^{(i)}(a_i, y) \otimes P^{(i)}(a_i, y) - I^{(i)} \otimes I^{(i)},$$

$I^{(i)}$ being the identity operator in $\mathcal{H}_i$. Using this identity and elementary properties of relative trace, equation (3.4) can be written as

$$\rho = \sum_{K \subseteq \{1, 2, \ldots, n\}} \alpha(K) S_p(K)$$

where

$$\alpha(K) = (d_1 d_2 \ldots d_n)^{-1} d(K) \sum_{L: L \cap K = \emptyset} (-1)^{|L|}|d'(L)|$$

Remark From Theorem 3.1 it is clear that $\rho$ is recovered from the probabilities for the elementary events

$$P^{(1)}(a_1, x_1) P^{(2)}(a_2, x_2) \ldots P^{(n)}(a_n, x_n), \quad a_i \in \mathbb{F}_{d_i}, x_i \in \mathbb{F}_{d_i}.$$
Acknowledgement: I wish to thank Professor S. Chaturvedi of the University of Hyderabad for bringing my attention to the central problem of this paper and the reference [7].

References

1. V. Arvind and K. R. Parthasarathy, *A family of quantum stabilizer codes based on the Weyl commutation relations over a finite field*, in A Tribute to C. S. Seshadri, Perspectives in Geometry and Representation Theory, Ed. V. Lakshmibai et al, Hindustan Book Agency, New Delhi (2003) 133-149.

2. V. Arvind, P. Kurur and K. R. Parthasarathy, *Nonstabilizer quantum codes from abelian subgroups of the error group*, quant-ph/0210097, to appear in Volume in honour of A. S. Holevo on his 60th birthday Ed. O. Hirota, 2004.

3. S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, *A new proof for the existence of mutually unbiased bases*, arXiv:quant-ph/0103162 v3, 7 Sept.2001.

4. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 1999.

5. K. R. Parthasarathy, *Lectures on quantum computation, quantum error-correcting codes and information theory* (Notes by Amitava Bhattacharyya, TIFR, Mumbai, 2003).

6. A. O. Pittenger and M. H. Rubin, *Mutually unbiased bases, generalized spin matrices and separability*, arXiv:quant-ph/0308142 v1, 26 August 2003.

7. W. K. Wooters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Annals of Physics, 191 (1989) No.2, 363-381.