

Mutually unbiased bases

S CHATURVEDI

School of Physics, University of Hyderabad, Hyderabad 500 046, India
Email: scsp@uohyd.ernet.in

Abstract. After a brief review of the notion of a full set of mutually unbiased bases in an N -dimensional Hilbert space, we summarize the work of Wootters and Fields (W K Wootters and B C Fields, *Ann. Phys.* **191**, 363 (1989)) which gives an explicit construction for such bases for the case $N = p^r$, where p is a prime. Further, we show how, by exploiting certain freedom in the Wootters–Fields construction, the task of explicitly writing down such bases can be simplified for the case when p is an odd prime. In particular, we express the results entirely in terms of the character vectors of the cyclic group G of order p . We also analyse the connection between mutually unbiased bases and the representations of G .

Keywords. Mutually unbiased bases; maximally noncommuting observables; optimal quantum state determination; Galois fields determination.

PACS Nos 03.65.Ta; 03.65.Wj

The notion of a full set of mutually unbiased bases, MUB's for short, in an N -dimensional Hilbert space may be viewed as an extension of the properties of the familiar Pauli matrices, $\sigma_x, \sigma_y, \sigma_z$ which arise in the description of the simplest quantum mechanical system – a spin-half system. For a spin-half particle, consider the observables $\hat{\mathbf{n}}_1 \cdot \sigma$ and $\hat{\mathbf{n}}_2 \cdot \sigma$, where $\hat{\mathbf{n}}_1$ and $\hat{\mathbf{n}}_2$ are real three-dimensional unit vectors. These, as is well-known, obey the commutation relations

$$[\hat{\mathbf{n}}_1 \cdot \sigma, \hat{\mathbf{n}}_2 \cdot \sigma] = i\hat{\mathbf{n}}_3 \cdot \sigma ; \quad \hat{\mathbf{n}}_3 = (\hat{\mathbf{n}}_1 \times \hat{\mathbf{n}}_2). \quad (1)$$

Clearly, these observables are 'maximally non-commuting' [1] when $\hat{\mathbf{n}}_1$ and $\hat{\mathbf{n}}_2$ are mutually orthogonal. Thus, the observables $\hat{\mathbf{n}}_i \cdot \sigma$, $i = 1, 2, 3$ with $\hat{\mathbf{n}}_i$'s as mutually orthogonal real unit vectors, and, in particular, $\sigma_x, \sigma_y, \sigma_z$ constitute a maximally non-commuting set in this sense. Consider now an arbitrary state of a spin-half particle which, as is well known, can be parametrized as

$$\rho = \frac{1}{2}(I + \mathbf{n} \cdot \sigma) ; \quad \mathbf{n} \cdot \mathbf{n} \leq 1. \quad (2)$$

To determine \mathbf{n} and hence ρ it is sufficient to consider any three observables $\hat{\mathbf{n}}_i \cdot \sigma$ with $\hat{\mathbf{n}}_i$'s non-coplanar. The vector \mathbf{n} can be reconstructed from expectation values $\langle \hat{\mathbf{n}}_i \cdot \sigma \rangle$ by solving the equations

$$\langle \hat{\mathbf{n}}_i \cdot \sigma \rangle = \hat{\mathbf{n}}_i \cdot \mathbf{n}; \quad i = 1, 2, 3. \quad (3)$$

However, if there are errors in the measurements, then it is intuitively obvious that the best strategy to determine ρ would be to choose \hat{n}_i as mutually orthogonal, i.e., to choose the observables to be ‘maximally non-commuting’. If we examine the normalized eigenvectors of such a set of observables then we find that we have three orthonormal sets of vectors with the property that the modulus square of the scalar product of a vector from any set with a vector from another set is $1/2$. For instance, the normalized eigenvectors of $\sigma_z, \sigma_x, \sigma_y$ are

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \quad (4)$$

as can easily be verified. An extension of this property, to arbitrary dimensions, leads to the following definition:

Definition. In a Hilbert space of dimension N , by a full set of mutually unbiased bases (MUB’s) we mean a set of $N + 1$ orthonormal bases such that the modulus square of the scalar product of any member of one basis with any member of any other basis is equal to $1/N$.

If we take $e^{(\alpha,k)}$ to denote the k th vector in the α th orthonormal basis, then having a full set of MUB’s amounts to having a collection $e^{(\alpha,k)}$; $\alpha = 0, 1, \dots, N$; $k = 0, 1, \dots, N - 1$, of $N(N + 1)$, N -dimensional complex vectors satisfying

$$\begin{aligned} |\langle e^{(\alpha,k)}, e^{(\alpha',k')} \rangle|^2 &\equiv \left| \sum_{l=0}^{N-1} (e_l^{(\alpha,k)})^* (e_l^{(\alpha',k')}) \right|^2 \\ &= \delta^{\alpha\alpha'} \delta^{kk'} + \frac{1}{N} (1 - \delta^{\alpha\alpha'}) ; \alpha, \alpha' = 0, 1, \dots, N ; \\ &k, k' = 0, 1, \dots, N - 1. \end{aligned} \quad (5)$$

Here $e_l^{(\alpha,k)}$ denotes the l th component of the k th vector belonging to the α th orthonormal basis.

Note that for any N , one of the $N + 1$ orthonormal bases, say, the one corresponding to $\alpha = N$ may always be chosen to be the standard basis

$$e_l^{(N,k)} = \delta_{lk}; \quad l, k = 0, 1, \dots, N - 1, \quad (6)$$

and we can, therefore, confine ourselves only to the remaining N orthonormal bases $e^{(m,k)}$ with both m and k running over $0, 1, \dots, N - 1$. These, of course, must not only be unbiased with respect to each other but must also be unbiased with respect to the standard basis. The latter requirement implies that $|e_l^{(m,k)}|$ should be equal to $1/\sqrt{N}$ for all m, k, l .

Mutually unbiased bases play an important role in quantum cryptography [2] and in the optimal determination of the density operator of an ensemble [3,4]. A density operator ρ in N -dimensions depends on $N^2 - 1$ real quantities. With the help of MUB’s, any such density operator can be encoded, in an optimal way, in terms of $N + 1$ sets of probability distributions each containing $N - 1$ independent probabilities [3,4]:

$$p^{(N,k)} = \rho_{kk}, \quad (7a)$$

$$p^{(m,k)} = \sum_{l,s} e_l^{(m,k)*} \rho_{ls} e_s^{(m,k)}. \quad (7b)$$

Conversely, from these probabilities one can reconstruct the density matrix using

$$\rho_{kk} = p^{(N,k)}, \quad (8a)$$

$$\rho_{ls} = \sum_{m,k} e_l^{(m,k)} p^{(m,k)} e_s^{(m,k)*}, l \neq s. \quad (8b)$$

Explicit construction of MUB's has been possible only for $N = p^r$ where p is a prime. The first construction of the set of MUB's for $N = p$ was given by Ivanovic [5] and later by Wootters [3]. Subsequently, Wootters and Fields [4] extended the construction in [3] to the case $N = p^r$ by making use of the properties of Galois fields [6]. (A recent work by Bandyopadhyay *et al* [7] contains an alternative construction for $N = p^r$ as well as a necessary and sufficient condition for the existence of MUB's for an arbitrary N).

A brief summary of the Wootters–Fields construction [4] is as follows

Case I: $N = p^r$, p : an odd prime

In this case

$$e_{\underline{l}}^{(\underline{m},\underline{k})} = \frac{1}{\sqrt{N}} \omega^{\text{Tr}[\underline{m}\underline{l}^2 + \underline{k}\underline{l}]} ; \quad \omega = e^{2\pi i/p}. \quad (9)$$

Here the symbols $\underline{m}, \underline{k}, \underline{l}$ which label bases, vectors in a given basis, and components of a given vector in a given basis, respectively, stand for r -dimensional arrays $(m_0, m_1, \dots, m_{r-1})$ etc. whose components take values in the set $0, 1, 2, \dots, p-1$, i.e., in the field \mathcal{Z}_p . Their boldfaced counterparts $\mathbf{m}, \mathbf{k}, \mathbf{l}$ which appear on the rhs of (9) belong to the Galois field $\text{GF}(p^r)$, i.e., they denote polynomials in x of degree r whose components in the basis $1, x, x^2, \dots, x^{r-1}$ are $(m_0, m_1, \dots, m_{r-1})$ etc. Thus $\underline{m} \longleftrightarrow \mathbf{m} \equiv m_0 + m_1 x + m_2 x^2 + \dots + m_{r-1} x^{r-1}$. The variable x is a root of a polynomial of degree r with coefficients in \mathcal{Z}_p and irreducible in \mathcal{Z}_p , i.e., with no roots in \mathcal{Z}_p . The trace operation on the rhs of (9) is defined as follows

$$\text{Tr}[\mathbf{m}] = \mathbf{m} + \mathbf{m}^2 + \dots + \mathbf{m}^{p^r-1}, \quad (10)$$

and takes elements of $\text{GF}(p^r)$ to elements of \mathcal{Z}_p . On carrying out the trace operation in (9) one obtains

$$e_{\underline{l}}^{(\underline{m},\underline{k})} = \frac{1}{\sqrt{N}} \omega^{\underline{m}^T \underline{q}(\underline{l})} \omega^{\underline{k}^T \underline{l}}. \quad (11)$$

The components of $\underline{q}(\underline{l})$ are given by

$$q_i(\underline{l}) = \underline{l}^T \beta_i \underline{l} \text{ mod } p, \quad i = 0, 1, 2, \dots, r-1, \quad (12)$$

where the $r \times r$ matrices β_i , $i = 0, 1, \dots, r-1$, are obtained from the multiplication table of $(1, x, x^2, \dots, x^{r-1})$:

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^{r-1} \end{pmatrix} (1 \quad x \quad \dots \quad x^{r-1}) = \beta_0 + \beta_1 x + \beta_2 x^2 + \dots + \beta_{r-1} x^{r-1}. \quad (13)$$

Case II: $N = 2^r$

As shown by Wootters and Fields, (11) works for $p = 2$ as well if we replace ω by i in the first factor on the RHS and suspend mod p operation while calculating $q_i(\underline{l})$ using (12).

Hereafter we will confine ourselves to Case I. We may rewrite (11) in terms of extended arrays $(\underline{m}, \underline{k})$ and $(\underline{q}(\underline{l}), \underline{l})$ as

$$e_{\underline{l}}^{(\underline{m}, \underline{k})} = \frac{1}{\sqrt{N}} \omega^{(\underline{m}, \underline{k})^T (\underline{q}(\underline{l}), \underline{l})}, \tag{14}$$

from which it is immediately obvious that if we take \underline{l} to label the rows and $(\underline{m}, \underline{k})$ to label the columns (arranged in a lexicographical order) of an $N \times N^2$ matrix e then the l th row of this matrix is given by

$$\begin{aligned} \frac{1}{\sqrt{N}} \chi^{(\underline{q}(\underline{l}), \underline{l})} &\equiv \frac{1}{\sqrt{N}} \chi^{(q_0(\underline{l}))} \otimes \chi^{(q_1(\underline{l}))} \otimes \dots \otimes \chi^{(q_{r-1}(\underline{l}))} \otimes \chi^{(l_0)} \otimes \chi^{(l_1)} \\ &\otimes \dots \otimes \chi^{(l_{r-1})}, \end{aligned} \tag{15}$$

where $\chi^{(l)}; l = 0, 1, \dots, p - 1$, denote the character vectors of the cyclic group G of order p . The matrix e contains the full set of MUB's – the constituent orthonormal bases are obtained by chopping this matrix into strips of width N . Of course, to write this matrix down explicitly one needs to work out $q(\underline{l})$ for each \underline{l} using (12).

We now suggest a simpler way of achieving the same results with much less work. First, we notice that the rows of e can be stacked on top of each other in any order. We will take the first row to correspond to $\underline{l} = \underline{0}$, i.e., as $\chi^{(\underline{0}, \underline{0})}$. To determine the remaining rows we proceed as follows. Choose the irreducible polynomial $f(x)$ in such a way that x is a primitive element of $\text{GF}^*(p^r) \equiv \text{GF}(p^r) \setminus \{0\}$. Its powers x, x^2, \dots, x^{p^r-1} then give all the information we need to write the matrix e .

As an illustration, consider the case $p = 5, r = 1$. Here $\text{GF}^*(5) = \mathcal{Z}_p^* = \{1, 2, 3, 4\}$. It is easy to see that 3 is a primitive element and that its powers modulo 5 are

$$3 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1, \tag{16}$$

which gives $l = 3 \rightarrow q(l) = 4, l = 4 \rightarrow q(l) = 1, l = 2 \rightarrow q(l) = 4, l = 1 \rightarrow q(l) = 1$, and hence

$$e = \frac{1}{\sqrt{5}} \begin{pmatrix} \chi^{(0)} \otimes \chi^{(0)} \\ \chi^{(1)} \otimes \chi^{(1)} \\ \chi^{(4)} \otimes \chi^{(2)} \\ \chi^{(4)} \otimes \chi^{(3)} \\ \chi^{(1)} \otimes \chi^{(4)} \end{pmatrix}. \tag{17}$$

As another example, consider for instance $p = 3, r = 2$. In this case $f(x) = x^2 + x + 2$ is a polynomial of degree 2 irreducible over \mathcal{Z}_3 such that x is a primitive element of the multiplicative abelian group $\text{GF}(3^2) \setminus \{0\}$ [8]. Computing the powers of x modulo $f(x)$ we obtain

$$\begin{aligned} x &= 0 + 1x, x^2 = 1 + 2x, x^3 = 2 + 2x, x^4 = 2 + 0x, x^5 = 0 + 2x, \\ x^6 &= 2 + x, x^7 = 1 + x, x^8 = 1 + 0x, \end{aligned} \tag{18}$$

which immediately gives the $\underline{l} \rightarrow \underline{q}(\underline{l})$ correspondence. Thus $x \equiv (0, 1) \rightarrow x^2 \equiv (1, 2); x^2 \equiv (1, 2) \rightarrow x^4 \equiv (2, 0)$ etc. and we have

$$e = \frac{1}{\sqrt{9}} \begin{pmatrix} \chi^{(0)} \otimes \chi^{(0)} \otimes \chi^{(0)} \otimes \chi^{(0)} \\ \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(1)} \\ \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(2)} \\ \chi^{(1)} \otimes \chi^{(0)} \otimes \chi^{(1)} \otimes \chi^{(0)} \\ \chi^{(2)} \otimes \chi^{(1)} \otimes \chi^{(1)} \otimes \chi^{(1)} \\ \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(1)} \otimes \chi^{(2)} \\ \chi^{(1)} \otimes \chi^{(0)} \otimes \chi^{(2)} \otimes \chi^{(0)} \\ \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(2)} \otimes \chi^{(1)} \\ \chi^{(2)} \otimes \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(2)} \end{pmatrix}. \quad (19)$$

Finally, it is natural to ask the question as to what relation, if any, exists between the MUB's and the representations of the cyclic group of order p . The answer to this question can be obtained by examining the two factors on the rhs of (11), and the following facts emerge:

- The diagonal matrices $\Omega^{(\underline{m})}$ with diagonal elements $\omega^{\underline{m}^T \underline{q}(\underline{l})}$ (\underline{l} taken as a row label) provide an $N = p^r$ -dimensional unitary reducible representation of the direct product group $G^r = G \times G \times \dots \times G$. This representation contains the trivial representation once together with half of the nontrivial irreducible representations which occur with multiplicity two.

Thus, for instance, for $p = 3, r = 1$, we have

$$\omega^{(0)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad \omega^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix}; \quad \omega^{(2)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad (20)$$

which clearly furnish a three-dimensional reducible representation of the cyclic group of order 3 in which the identity representation occurs once and one of the two non-trivial representation occurs twice.

- The diagonal matrices $\mathcal{R}^{(\underline{k})}$ with diagonal elements $\omega^{\underline{k}^T \underline{l}}$ (\underline{l} taken as a row label) provide an $N = p^r$ -dimensional unitary reducible representation of the direct product group $G^r = G \times G \times \dots \times G$ which contains all the irreducible representations once (the regular representation). Thus, for instance, for $p = 3, r = 1$, we have

$$\omega^{(0)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad \omega^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}; \quad \omega^{(2)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix}, \quad (21)$$

which clearly furnish a three-dimensional reducible representation of the cyclic group of order 3 in which all the representations occur once.

- The diagonal matrices $\Omega^{(\underline{m})} \mathcal{R}^{(\underline{k})}$ provide an $N = p^r$ -dimensional unitary reducible representation of the direct product group $G^r \times G^r$ in which certain prescribed irreducible representations occur only once. This representation essentially yields the MUB's in odd prime power dimensions.

Consider, again, the case $p = 3, r = 1$. Pairwise products of the matrices above give us nine matrices which furnish a three-dimensional reducible representation of the direct product group of the cyclic group of order 3 with itself. The diagonals of these matrices give us the nine vectors in the MUB for $N = 3$ (apart from the three in the standard basis).

To conclude, we have shown that the freedom in the choice of the irreducible polynomial $f(x)$ in carrying out the computations in (6) and (7) can be profitably exploited to simplify the task by choosing to work with an $f(x)$ whose roots are primitive elements of $\text{GF}^*(p^r)$. We have also brought out the connection between the MUB's for $N = p^r$ and the representations of the cyclic group of order p . The question of existence of MUB's in dimensions other than $N = p^r$ is an interesting open problem worthy of further investigations.

Acknowledgements

I am grateful to Prof. J Pasupathy for introducing me to the subject of MUB's.

References

- [1] J Schwinger, *Proc. Natl. Acad. Sci. U.S.A.* **46**, 570 (1960)
- [2] H Bechmann-Pasquinucci and A Peres, *Phys. Rev. Lett.* **85**, 3313 (2000)
- [3] W K Wootters, *Found. Phys.* **16**, 391 (1986)
- [4] W K Wootters and B C Fields, *Ann. Phys.* **191**, 363 (1989)
- [5] I D Ivanovic, *J. Phys.* **A14**, 3241 (1981); *J. Math. Phys.* **24**, 1199 (1983)
- [6] See, for instance, R Lidl and G Pilz, *Applied abstract algebra* (Springer Verlag, New York, Berlin, Heidelberg, Tokyo, 1984)
- [7] S Bandyopadhyay, P Oscar Boykin, V Roychowdhury and F Vatan, quant-ph/0103162
- [8] Lists of irreducible polynomials for low values of p and r together with the order of their roots may be found in [6]. For given p and r , the number of such polynomials is equal to $\phi(p^r - 1)/r$, where ϕ is the Euler phi-function