Aspects of mutually unbiased bases in odd-prime-power dimensions

S. Chaturvedi*
School of Physics, University of Hyderabad, Hyderabad 500046, India
(Received 4 September 2001; published 21 March 2002)

We rephrase the Wootters-Fields construction [W. K. Wootters and B. C. Fields, Ann. Phys. **191**, 363 (1989)] of a full set of mutually unbiased bases in a complex vector space of dimensions $N=p^r$, where p is an odd prime, in terms of the character vectors of the cyclic group G of order p. This form may be useful in explicitly writing down mutually unbiased bases for $N=p^r$.

DOI: 10.1103/PhysRevA.65.044301 PACS number(s): 03.65.Ta

In a complex vector space of dimension N, by a full set of mutually unbiased bases (MUBs) 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 kth vector in the αth orthonormal basis, then having a full set of MUBs amounts to having a collection $e^{(\alpha,k)}$; $\alpha=0,1,\ldots,N$; $k=0,1,\ldots,N-1$ of $N(N+1)$, N-dimensional complex vectors satisfying

$$|\langle e^{(\alpha,k)},e^{(\alpha',k')}\rangle|^2\equiv\left|\sum_{l=0}^{N-1}(e_l^{(\alpha,k)})^*(e_l^{(\alpha',k')})\right|^2$$

$$=\delta^{\alpha\alpha'}\delta^{kk'}+\frac{1}{N}(1-\delta^{\alpha\alpha'});$$

$$\alpha,\alpha'=0,1,\ldots,$$

$$N;k,k'=0,1,\ldots,N-1. \tag{1}$$

Here $e_l^{\{\alpha,k\}}$ denotes the lth component of the kth vector belonging to the αth orthonormal basis. Mutually unbiased bases, thus, generalize the properties of the eigenvectors of the familiar Pauli matrices $\sigma_x,\sigma_y,\sigma_z$.

Though the notion of a pair of mutually unbiased bases as corresponding to a pair of ''maximally noncommuting'' measurements was introduced by Schwinger [1] as early as 1960, explicit construction of a full set of MUBs for $N=p$ was first given by Ivanovic [2] 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 [5]. In this work, Wootters and Fields, also clearly brought out the relevance of the MUBs for an optimal determination of the density matrix of an ensemble. It is this aspect of MUBs that underlies their usefulness in quantum estimation theory and in quantum cryptography [6]. A recent work by Bandyopadhyay *et al.* [7] contains, among other interesting results, an explicit construction of the unitary matrices (analogs of the Pauli matrices in $N=p^r$ dimensions) whose eigenvectors provide a full set of MUBs.

The purpose of this paper is to show that, by exploiting certain freedom inherent to the Wootters-Fields construction, the task of explicitly writing down the the full set of MUBs in odd-prime-power dimensions can be considerably simplified.

We begin by noting 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

$$e_l^{(N,k)}=\delta_{lk},\quad l,k=0,1,\ldots,N-1, \tag{2}$$

and we can, therefore, confine ourselves only to the remaining N orthonormal bases $e^{(m,k)}$ with both m and k running over $0,1,\ldots,N-1$. 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.

As noted above, explicit construction of a full set of MUBs has so far been possible for $N=p^r$, p is a prime. For the case when p is odd, one has [4]

$$e_l^{(m,k)}=\frac{1}{\sqrt{N}}\omega^{\mathrm{Tr}[\mathbf{ml}^2+\mathbf{kl}]};\quad \omega=e^{2\pi i/p}. \tag{3}$$

Here the symbols m, k, and 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 $(m_0,m_1,\ldots,m_{r-1})$ etc. whose components take values in the set $0,1,2,\ldots,p-1$, i.e., in the field $\mathcal{Z}_p$. Their boldfaced counterparts $\mathbf{m}$, $\mathbf{k}$, and $\mathbf{l}$ which appear on the right-hand side (rhs) of Eq. (3) belong to the Galois field GF(p^r), i.e., they denote polynomials in x of degree r whose components in the basis $1,x,x^2,\ldots,x^{r-1}$ are $(m_0,m_1,\ldots,m_{r-1})$ etc. Thus, $m\leftrightarrow\mathbf{m}\equiv m_0+m_1x+m_2x^2+\cdots,m_{r-1}x^{r-1}$. 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 Eq. (3) is defined as follows:

$$\mathrm{Tr}[\mathbf{m}]=\mathbf{m}+\mathbf{m}^2+\cdots,\mathbf{m}^{p^{r-1}}, \tag{4}$$

and takes elements of GF(p^r) to elements of $\mathcal{Z}_p$. On carrying out the trace operation in Eq. (3) one obtains

$$e_l^{(m,k)}=\frac{1}{\sqrt{N}}\omega^{m^Tq(l)}\omega^{k^Tl}. \tag{5}$$

The components of $q(l)$ are given by

*Email address: scsp@uohyd.ernet.in

$$q_i(l) = l^T \beta_i l \bmod p, \quad i = 0,1,2,\ldots,r-1, \tag{6}$$

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

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^{r-1} \end{pmatrix} (1x\cdots x^{r-1}) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_{r-1} x^{r-1}. \tag{7}$$

[As shown by Wootters and Fields, Eq. (5) 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 $q_i(l)$ using Eq. (6).]

We may rewrite Eq. (5) in terms of extended arrays (m,k) and $(q(l),l)$ as

$$e_l^{(m,k)} = \frac{1}{\sqrt{N}} \omega^{(m,k)^T (q(l),l)}, \tag{8}$$

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

$$\frac{1}{\sqrt{N}} \chi^{(q(l),l)} \equiv \frac{1}{\sqrt{N}} \chi^{(q_0(l))} \otimes \chi^{(q_1(l))} \cdots \otimes \chi^{(q_{r-1}(l))} \otimes \chi^{(l_0)} \otimes \chi^{(l_1)} \otimes \cdots \otimes \chi^{(l_{r-1})}, \tag{9}$$

where $\chi^{(l)}$; $l = 0,1,\ldots,p-1$ denote the character vectors of the cyclic group G of order p. The matrix e contains the full set of MUBs—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 $q(l)$ for each l using Eq. (6). 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 $l=0$, i.e., as $\chi^{(0,0)}$. 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 $\mathrm{GF}^*(p^r) \equiv \mathrm{GF}(p^r) \setminus \{0\}$. Its powers $x, x^2, \ldots, x^{p^r-1}$ then give all the information we need to write the matrix e.

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

$$3 = 3, \quad 3^2 = 4, \quad 3^3 = 2, \quad 3^4 = 1, \tag{10}$$

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

$$e = \frac{1}{\sqrt{5}} \begin{pmatrix} \chi^{(0)} \otimes \chi^{(0)} \\ \chi^{(1)} \otimes \chi^{(1)} \\ \chi^{(4)} \otimes \chi^{(2)} \\ \chi^{(4)} \otimes \chi^{(3)} \\ \chi^{(1)} \otimes \chi^{(4)} \end{pmatrix}. \tag{11}$$

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 $\mathcal{Z}_3$ and such that x is a primitive element of the multiplicative abelian group $\mathrm{GF}(3^2) \setminus \{0\}$ [8]. Computing the powers of x modulo $f(x)$ we obtain

$$x = 0 + 1x, \quad x^2 = 1 + 2x, \quad x^3 = 2 + 2x, \quad x^4 = 2 + 0x,$$
$$x^5 = 0 + 2x, \quad x^6 = 2 + x, \quad x^7 = 1 + x, \quad x^8 = 1 + 0x, \tag{12}$$

which immediately gives the $l \to q(l)$ correspondences. Thus, $x \equiv (0,1) \to x^2 \equiv (1,2); x^2 \equiv (1,2) \to x^4 \equiv (2,0)$ etc. and we have

$$e = \frac{1}{\sqrt{9}} \begin{pmatrix} \chi^{(0)} \otimes \chi^{(0)} \otimes \chi^{(0)} \otimes \chi^{(0)} \\ \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(1)} \\ \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(2)} \\ \chi^{(1)} \otimes \chi^{(0)} \otimes \chi^{(1)} \otimes \chi^{(0)} \\ \chi^{(2)} \otimes \chi^{(1)} \otimes \chi^{(1)} \otimes \chi^{(1)} \\ \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(1)} \otimes \chi^{(2)} \\ \chi^{(1)} \otimes \chi^{(0)} \otimes \chi^{(2)} \otimes \chi^{(0)} \\ \chi^{(2)} \otimes \chi^{(0)} \otimes \chi^{(2)} \otimes \chi^{(1)} \\ \chi^{(2)} \otimes \chi^{(1)} \otimes \chi^{(2)} \otimes \chi^{(2)} \end{pmatrix}. \tag{13}$$

Some interesting features that become explicit by examining the two factors on the rhs of Eq. (5) are listed below.

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

The diagonal matrices $\mathcal{R}^{(k)}$ with diagonal elements $\omega^{k^T l}$ (l taken as a row label) provide an $N = p^r$ dimensional unitary reducible representation of the direct product group $G^r = G \times G \times \cdots \times G$ that contains all the irreducible representations once (the regular representation).

The diagonal matrices $\Omega^{(m)} \mathcal{R}^{(k)}$ 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 MUBs in odd-prime-power dimensions.

To conclude, we have shown that the freedom in the choice of the irreducible polynomial $f(x)$ in carrying out the computations in Eqs. (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 $\mathrm{GF}^*(p^r)$.

[1] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).
[2] I.D. Ivanovic, J. Phys. A **14**, 3241 (1981); J. Math. Phys. **24**, 1199 (1983).
[3] W.K. Wootters, Found. Phys. **16**, 391 (1986).
[4] W.K. Wootters and B.C. Fields, Appl. Phys. **191**, 363 (1989).
[5] See, for instance, R. Lidl and G. Pilz, *Applied Abstract Algebra* (Springer-Verlag, New York, 1984).
[6] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[7] S. Bandyopadhyay, P. Oscar Boykin, V. Roychowdhury, and F. Vatan, e-print 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 [5].