

Max-Planck-Institut
für Mathematik
in den Naturwissenschaften
Leipzig

Unextendible maximally entangled bases and
mutually unbiased bases

by

Bin Chen and Shao-Ming Fei

Preprint no.: 8

2014



Unextendible maximally entangled bases and mutually unbiased bases

Bin Chen¹ and Shao-Ming Fei^{1,2}

¹*School of Mathematical Sciences, Capital Normal University, Beijing 100048, China*

²*Max-Planck-Institute for Mathematics in the Sciences, 04103 Leipzig, Germany*

We study unextendible maximally entangled basis in arbitrary bipartite spaces. A systematic way of constructing a set of d^2 orthonormal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ ($\frac{d'}{2} < d < d'$) is provided. The complementary space of the set of these d^2 orthonormal maximally entangled states contains no maximally entangled states that are orthogonal to all of them. Furthermore, we investigate mutually unbiased bases in which all the bases are unextendible maximally entangled ones. We present two unextendible maximally entangled bases in $\mathbb{C}^2 \otimes \mathbb{C}^3$ which are mutually unbiased.

PACS numbers:

I. INTRODUCTION

Quantum entanglement plays vital roles in quantum information processing and has been extensively investigated in recent years [1, 2]. It is the difference between entangled and product quantum states that gives rise to the intrinsic distinction of quantum mechanics, as well as some fundamental problems related to the quantum mechanics such as reality and non-locality. It has been shown that there could be sets of product states which nevertheless display a form of nonlocality [3, 4].

Considerable theoretical results with useful applications have been obtained, ever since the concept of unextendible product basis (UPB) in multipartite quantum systems has been introduced in [3]. The UPB is a set of incomplete orthonormal product basis whose complementary space has no product states. It is shown that the mixed state on the subspace complementary to a UPB is a bound entangled state. Moreover, the states comprising a UPB are not distinguishable by local measurements and classical communication.

The UPB is generalized to unextendible maximally entangled basis (UMEB) [5]: a set of orthonormal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ consisting of fewer than d^2 vectors which have no additional maximally entangled vectors orthogonal to all of them. It has been shown that there does not exist UMEBs for $d = 2$. Explicit examples are presented a 6-member UMEB for $d = 3$ and a 12-member UMEB for $d = 4$.

Another interestingly related problem is the mutually unbiased base (MUB). Two orthonormal bases $\mathcal{B}_1 = \{|b_i\rangle\}_{i=1}^d$ and $\mathcal{B}_2 = \{|c_j\rangle\}_{j=1}^d$ of \mathbb{C}^d are said to be mutually unbiased (MU) if and only if

$$|\langle b_i | c_j \rangle| = \frac{1}{\sqrt{d}}, \quad \forall i, j = 1, 2, \dots, d.$$

If a physical system is prepared in an eigenstate of basis \mathcal{B}_1 and measured in basis \mathcal{B}_2 , then all outcomes are equally probable. A set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m\}$ in \mathbb{C}^d is called a set of mutually unbiased bases (MUBs) if every pair of bases in the set is mutually unbiased.

MUBs have useful applications in many quantum information processing, such as quantum state tomography [6–8], cryptographic protocols [9, 10], and the mean kings problem [11]. The maximum number $N(d)$ of MUBs is no more than $d + 1$. It has been shown that $N(d) = d + 1$ when d is a prime power [6]. However, when d is a composite number, $N(d)$ is still unknown. Even for $d = 6$, we do not know whether there exist four MUBs or not [12–15]. Hence the research on $N(6)$ and construction of MUBs in \mathbb{C}^6 is of great importance.

In this paper, we first study UMEB in arbitrary bipartite spaces $\mathbb{C}^d \otimes \mathbb{C}^{d'}$. We provide a systematic way in constructing d^2 -member UMEBs in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ ($\frac{d'}{2} < d < d'$). We show that the subspace complementary to the d^2 -member UMEB contains no states of Schmidt rank higher than $d - 1$. Thus we answer the question proposed by S. Bravyi and J. A. Smolin in [5] whether there exist any “nonsquare” UMEBs, i.e. UMEBs in the bipartite spaces with different dimensions. Moreover, we construct two complete UMEBs in $\mathbb{C}^2 \otimes \mathbb{C}^3$ which are mutually unbiased.

II. UMEBS IN $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ ($\frac{d'}{2} < d < d'$)

We first study unextendible maximally entangled basis in bipartite spaces with different dimensions.

Definition. A set of states $\{|\phi_i\rangle \in \mathbb{C}^d \otimes \mathbb{C}^{d'} : i = 1, 2, \dots, n, n < dd'\}$ is called an n -number UMEB if and only if

- (i) $|\phi_i\rangle, i = 1, 2, \dots, n$, are maximally entangled;
- (ii) $\langle \phi_i | \phi_j \rangle = \delta_{ij}$;
- (iii) if $\langle \phi_i | \psi \rangle = 0$ for all $i = 1, 2, \dots, n$, then $|\psi\rangle$ cannot be maximally entangled.

Here state $|\psi\rangle$ is said to be a $d \otimes d'$ maximally entangled state if and only if for arbitrary given orthonormal complete basis $\{|i_A\rangle\}$ of subsystem A, there exists an orthonormal basis $\{|i_B\rangle\}$ of subsystem B such that $|\psi\rangle$ can be written as $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i_A\rangle \otimes |i_B\rangle$ [16].

We first construct UMEB in $\mathbb{C}^2 \otimes \mathbb{C}^3$, then generalize the construction to the case in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ ($\frac{d'}{2} < d < d'$). Consider the following four maximally entangled states

in $\mathbb{C}^2 \otimes \mathbb{C}^3$:

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0'\rangle + |1\rangle|1'\rangle), \\ |\phi_i\rangle &= (\sigma_i \otimes I_3)|\phi_0\rangle, \quad i = 1, 2, 3, \end{aligned} \quad (1)$$

where $\{|0\rangle, |1\rangle\}, \{|0'\rangle, |1'\rangle, |2'\rangle\}$ are the orthonormal bases in \mathbb{C}^2 and \mathbb{C}^3 respectively, $\sigma_i, i = 1, 2, 3$, are the Pauli matrices. It can be easily checked that the above four states are mutually orthogonal. Now we prove that if there exists $|\psi\rangle$ such that $\langle\phi_i|\psi\rangle = 0, \forall i = 0, 1, 2, 3$, then $|\psi\rangle$ must be a product state.

$|\psi\rangle$ can be generally written in the Schmidt decomposition form,

$$|\psi\rangle = (U \otimes V)(\sqrt{\lambda_0}|0\rangle|0'\rangle + \sqrt{\lambda_1}|1\rangle|1'\rangle), \quad (2)$$

where $\lambda_0 > 0, \lambda_1 > 0, \lambda_0 + \lambda_1 = 1, U$ and V are unitary operators, $U = (u_{ij})_{2 \times 2}, V = (v_{ij})_{3 \times 3}$ in the ordered bases $\{|0\rangle, |1\rangle\}$ and $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ respectively.

The orthogonal relations between $|\psi\rangle$ and $|\phi_i\rangle$ give rise to the following equations:

$$\begin{aligned} \sqrt{\lambda_0}\langle 0|\sigma_i U|0\rangle\langle 0'|V|0'\rangle + \sqrt{\lambda_1}\langle 0|\sigma_i U|1\rangle\langle 0'|V|1'\rangle \\ + \sqrt{\lambda_0}\langle 1|\sigma_i U|0\rangle\langle 1'|V|0'\rangle + \sqrt{\lambda_1}\langle 1|\sigma_i U|1\rangle\langle 1'|V|1'\rangle = 0, \end{aligned}$$

$i = 0, 1, 2, 3$, where $\sigma_0 = I_2$. Hence we have

$$\begin{aligned} \sqrt{\lambda_0}u_{11}v_{11} + \sqrt{\lambda_1}u_{12}v_{12} + \sqrt{\lambda_0}u_{21}v_{21} + \sqrt{\lambda_1}u_{22}v_{22} &= 0, \\ \sqrt{\lambda_0}u_{21}v_{11} + \sqrt{\lambda_1}u_{22}v_{12} + \sqrt{\lambda_0}u_{11}v_{21} + \sqrt{\lambda_1}u_{12}v_{22} &= 0, \\ \sqrt{\lambda_0}u_{11}v_{11} + \sqrt{\lambda_1}u_{12}v_{12} - \sqrt{\lambda_0}u_{21}v_{21} - \sqrt{\lambda_1}u_{22}v_{22} &= 0, \\ \sqrt{\lambda_0}u_{21}v_{11} + \sqrt{\lambda_1}u_{22}v_{12} - \sqrt{\lambda_0}u_{11}v_{21} - \sqrt{\lambda_1}u_{12}v_{22} &= 0. \end{aligned}$$

The set of above equations can be expressed as $M\vec{v} = \vec{0}$, where

$$M = \begin{pmatrix} U & AU \\ U & -AU \end{pmatrix} \begin{pmatrix} W & \\ & W \end{pmatrix},$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad W = \begin{pmatrix} \sqrt{\lambda_0} & \\ & \sqrt{\lambda_1} \end{pmatrix},$$

and

$$\vec{v} = (v_{11}, v_{12}, v_{21}, v_{22})^T,$$

where T denotes matrix transpose.

Since $\det M \neq 0$, we obtain $\vec{v} = \vec{0}$, which implies that $\det V = 0$, and hence V cannot be unitary. Thus (1) is a 4-member UMEB in $\mathbb{C}^2 \otimes \mathbb{C}^3$, whose complementary space contains no entangled states.

We now construct UMEBs in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$, $\frac{d'}{2} < d < d'$, by using the approach for the case of $\mathbb{C}^2 \otimes \mathbb{C}^3$. Let $\{|i\rangle\}_{i=0}^{d-1}$ and $\{|i'\rangle\}_{i=0}^{d'-1}$ be orthonormal bases of \mathbb{C}^d and $\mathbb{C}^{d'}$ respectively. Consider a set of unitary operators, which forms a basis of the operator space on \mathbb{C}^d :

$$U_{nm} = \sum_{k=0}^{d-1} \zeta_d^{nk} |k \oplus m\rangle\langle k|, \quad n, m = 0, 1, \dots, d-1, \quad (3)$$

where $\zeta_d = e^{\frac{2\pi\sqrt{-1}}{d}}$, $k \oplus m$ denotes $(k+m) \bmod d$. These operators satisfy

$$\text{Tr}(U_{n'm'}^\dagger U_{nm}) = d \delta_{n'n} \delta_{m'm}.$$

Applying this set of unitary operators to the first party of a given maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$, we get d^2 mutually orthonormal maximally entangled states:

$$|\Phi_{nm}\rangle = (U_{nm} \otimes I_{d'})|\Phi\rangle, \quad n, m = 0, 1, \dots, d-1, \quad (4)$$

where $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} |p\rangle|p'\rangle$. We now prove that if there exists $|\Psi\rangle$ in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$, $\frac{d'}{2} < d < d'$, such that $\langle\Phi_{nm}|\Psi\rangle = 0$ for all n, m , then $|\Psi\rangle$ cannot be of Schmidt rank d , i.e. $|\Psi\rangle$ must not be maximally entangled.

$|\Psi\rangle$ can generally written as

$$|\Psi\rangle = (U \otimes V) \sum_{p=0}^{d-1} \sqrt{\lambda_p} |p\rangle|p'\rangle,$$

where $\lambda_p > 0$ for all $p, \sum_{p=0}^{d-1} \lambda_p = 1, U = (u_{ij})_{d \times d}$ and $V = (v_{ij})_{d' \times d'}$ are unitary matrices in the given ordered bases respectively. If $\langle\Phi_{nm}|\Psi\rangle = 0$ for all n and m , one gets d^2 equations:

$$\begin{aligned} \langle\Phi_{nm}|\Psi\rangle &= \frac{1}{\sqrt{d}} \sum_{k,p} \zeta_d^{-nk} \sqrt{\lambda_p} \langle k \oplus m|U|p\rangle \langle k'|V|p'\rangle \\ &= 0, \quad n, m = 0, 1, \dots, d-1. \end{aligned} \quad (5)$$

These equations can be expressed in a compact form: $M\vec{v} = \vec{0}$, where

$$M = \begin{pmatrix} U & AU & A^2U & \dots & A^{d-1}U \\ U & \zeta_d^{-1}AU & \zeta_d^{-2}A^2U & \dots & \zeta_d^{-(d-1)}A^{d-1}U \\ U & \zeta_d^{-2}AU & \zeta_d^{-4}A^2U & \dots & \zeta_d^{-2(d-1)}A^{d-1}U \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ U & \zeta_d^{-(d-1)}AU & \zeta_d^{-2(d-1)}A^2U & \dots & \zeta_d^{-(d-1)^2}A^{d-1}U \end{pmatrix} \begin{pmatrix} W & & & & \\ & W & & & \\ & & W & & \\ & & & \ddots & \\ & & & & W \end{pmatrix},$$

A is a permutation matrix,

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$M = \begin{pmatrix} I & I & I & \cdots & I \\ I & \zeta_d^{-1}I & \zeta_d^{-2}I & \cdots & \zeta_d^{-(d-1)}I \\ I & \zeta_d^{-2}I & \zeta_d^{-4}I & \cdots & \zeta_d^{-2(d-1)}I \\ \vdots & \vdots & \vdots & & \vdots \\ I & \zeta_d^{-(d-1)}I & \zeta_d^{-2(d-1)}I & \cdots & \zeta_d^{-(d-1)^2}I \end{pmatrix} \begin{pmatrix} I & & & & \\ & A & & & \\ & & A^2 & & \\ & & & \ddots & \\ & & & & A^{d-1} \end{pmatrix} \begin{pmatrix} U & & & & \\ & U & & & \\ & & \ddots & & \\ & & & U & \\ & & & & U \end{pmatrix} \begin{pmatrix} W & & & & \\ & W & & & \\ & & W & & \\ & & & \ddots & \\ & & & & W \end{pmatrix},$$

it is easily verified that $\det M \neq 0$, which implies that $\vec{v} = \vec{0}$. Due to that $d' < 2d$, we have $\det V = 0$ and V cannot be unitary. Therefore the d^2 mutually orthonormal maximally entangled states (4) constitute a d^2 -member UMEB in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ for $\frac{d'}{2} < d < d'$.

Like the UMEBs in $\mathbb{C}^d \otimes \mathbb{C}^d$, our ‘‘nonsquare’’ UMEBs have also interesting and useful applications in quantum information processing. For example, as it has been noted in [5], the relation of the complementary space to unital channels would be broken. Let $\{|\Phi_i\rangle : i = 1, 2, \dots, d^2\}$ be the set of d^2 -member UMEB constructed above in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$, $\frac{d'}{2} < d < d'$. The state

$$\rho^\perp = \frac{1}{dd' - d^2} (I - \sum_{i=1}^{d^2} |\Phi_i\rangle\langle\Phi_i|), \quad (6)$$

on a $d \otimes d'$ bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to a completely positive map $\Lambda : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_B)$ by Jamiołkowski isomorphism [16], and Λ is a quantum channel since $\text{Tr}_B(\rho^\perp) = \frac{1}{d}I_d$. But the corresponding channel would not be unital since

$$\text{Tr}_A(\rho^\perp) = \frac{1}{d' - d} (I_{d'} - \sum_{i=0}^{d-1} |i'\rangle\langle i'|) \neq \frac{1}{d'}I_{d'}.$$

Besides, as ρ^\perp cannot be a mixture of maximally entangled states, Λ cannot be convex mixtures of unitary operators.

III. MUBS FROM UMEBS IN $\mathbb{C}^2 \otimes \mathbb{C}^3$

MUBs, UPBs and UMEBs have significant applications in quantum information processing. In this section we study the possibility that all the bases in MUBs are also UMEBs. We construct two UMEBs in $\mathbb{C}^2 \otimes \mathbb{C}^3$ which are mutually unbiased.

$W = \text{diag}\{\sqrt{\lambda_0}, \sqrt{\lambda_1}, \dots, \sqrt{\lambda_{d-1}}\}$, $\vec{v} = (v_{11}, v_{12}, \dots, v_{1d}, v_{21}, v_{22}, \dots, v_{2d}, \dots, v_{d1}, v_{d2}, \dots, v_{dd})^T$. Since M can further written as

By using (1) we have the first UMEB in $\mathbb{C}^2 \otimes \mathbb{C}^3$:

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0'\rangle + |1\rangle|1'\rangle), \\ |\phi_i\rangle &= (\sigma_i \otimes I_3)|\phi_0\rangle, \quad i = 1, 2, 3, \\ |\phi_4\rangle &= (\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle) \otimes |2'\rangle, \\ |\phi_5\rangle &= (\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle) \otimes |2'\rangle. \end{aligned} \quad (7)$$

Starting with another basis in \mathbb{C}^3 :

$$\begin{aligned} |x'\rangle &= \frac{1}{\sqrt{3}}(|0'\rangle + \frac{1+\sqrt{3}i}{2}|1'\rangle + |2'\rangle), \\ |y'\rangle &= \frac{1}{\sqrt{3}}(\frac{-\sqrt{3}+i}{2}|0'\rangle + i|1'\rangle - i|2'\rangle), \\ |z'\rangle &= \frac{1}{\sqrt{3}}(-|0'\rangle + |1'\rangle + \frac{1+\sqrt{3}i}{2}|2'\rangle), \end{aligned}$$

where $i = \sqrt{-1}$, we can construct another UMEB in $\mathbb{C}^2 \otimes \mathbb{C}^3$,

$$\begin{aligned} |\psi_j\rangle &= \frac{1}{\sqrt{2}}(\sigma_j \otimes I_3)(|0\rangle|x'\rangle + |1\rangle|y'\rangle), \quad j = 0, 1, 2, 3, \\ |\psi_4\rangle &= \frac{1}{\sqrt{2}}(\frac{1+\sqrt{3}i}{2}|0\rangle + \frac{\sqrt{3}-i}{2}|1\rangle) \otimes |z'\rangle, \\ |\psi_5\rangle &= \frac{1}{\sqrt{2}}(\frac{\sqrt{3}-i}{2}|0\rangle + \frac{1+\sqrt{3}i}{2}|1\rangle) \otimes |z'\rangle. \end{aligned} \quad (8)$$

It is directly verified that the above two bases (7) and (8) are mutually unbiased.

IV. CONCLUSION AND DISCUSSION

We have studied UMEB in arbitrary bipartite spaces, and provided explicit construction of UMEBs in

$\mathbb{C}^d \otimes \mathbb{C}^{d'}$ ($d'/2 < d < d'$). We are not sure if there exist UMEBs in $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ for $d \leq d'/2$, and whether in this case the set of d^2 -member orthonormal maximally entangled basis we constructed is unextendible or not. If they are unextendible, one gets that the entanglement of assistance (EoA) [17] is strictly smaller than the asymptotic EoA [18] as the UMEBs do in $\mathbb{C}^d \otimes \mathbb{C}^d$ [5]. In fact, the asymptotic EoA of ρ^\perp in (6) is equal to $\log d$ when $d \leq d'/2$, since $S(\text{Tr}_A \rho^\perp) = \log(d' - d) \geq S(\text{Tr}_B \rho^\perp) =$

$\log d$, and the EoA of ρ^\perp is strictly smaller than $\log d$.

Moreover, we have presented two UMEBs in $\mathbb{C}^2 \otimes \mathbb{C}^3$ which are mutually unbiased. It would be interesting to investigate the implications and applications in quantum state tomography and cryptographic protocols for such MUBs in which all the bases are UMEBs.

Acknowledgments This work is supported by the NSFC under number 11275131.

-
- [1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).
- [2] O. Guhne, G. Toth, *Phys. Rep.* **474**, 1(2009).
- [3] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, *Phys. Rev. Lett.* **82**, 5385 (1999).
- [4] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, *Commun. Math. Phys.* **238**, 379 (2003).
- [5] S. Bravyi, and J. A. Smolin, *Phys. Rev. A* **84**, 042306 (2011).
- [6] W. K. Wootters and B. D. Fields, *Ann. Phys. (N.Y.)* **191**, 363 (1989).
- [7] R. B. A. Adamson and A. M. Steinberg, *Phys. Rev. Lett.* **105**, 030406 (2010).
- [8] A. Fernández-Pérez, A. B. Klimov, and C. Saavedra, *Phys. Rev. A* **83**, 052332 (2011).
- [9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [10] I.-C. Yu, F.-L. Lin, and C.-Y. Huang, *Phys. Rev. A* **78**, 012344 (2008).
- [11] B.-G. Englert and Y. Aharonov, *Phys. Lett. A* **284**, 1 (2001).
- [12] S. Brierley and S. Weigert, *Phys. Rev. A* **78**, 042312 (2008).
- [13] S. Brierley and S. Weigert, *Phys. Rev. A* **79**, 052316 (2009).
- [14] P. Raynal, X. Lü, and B.-G. Englert, *Phys. Rev. A* **83**, 062303 (2011).
- [15] D. McNulty and S. Weigert, *J. Phys. A: Math. Theor.* **45** 102001 (2012).
- [16] A. Jamiolkowski, *Rep. Math. Phys.* **3**, 275 (1972).
- [17] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. V. Thapliyal, and A. Uhlmann, in *Proceedings of Quantum Computing and Quantum Communications: First NASA International Conference, Palm Springs, 1998*, Springer Lecture Notes in Computer Science, Vol. 1509 (Springer, Heidelberg, 1999), pp. 247-257.
- [18] J. A. Smolin, F. Verstraete, and A. Winter, *Phys. Rev. A* **72**, 052317 (2005).