Unextendible Mutually Unbiased Bases in Prime-Squared Dimensions

Vishakh Hegde and Prabha Mandayam
Department of Physics, IIT Madras, Chennai - 600036, India
(Dated: November 25, 2014)

Two orthonormal bases $\mathcal{A} = \{|a_i\rangle, i = 1, \ldots, d\}$ and $\mathcal{B} = \{|b_j\rangle, j = 1, \ldots, d\}$ of a d-dimensional Hilbert space $\mathbb{C}^d$ are said to be **mutually unbiased** if for all basis vectors $|a_i\rangle \in \mathcal{A}$ and $|b_j\rangle \in \mathcal{B}$,

$$|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}, \forall i, j = 1, \ldots, d.$$

In other words, if a physical system is prepared in an eigenstate of basis $\mathcal{A}$ and measured in basis $\mathcal{B}$, all outcomes are equally probable. A set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ 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 form a minimal and optimal set of orthogonal measurements for quantum state tomography [1, 2]. Such bases play an important role in our understanding of complementarity in quantum mechanics [3] and are central to quantum information tasks such as entanglement detection [4], information locking [5], and quantum cryptography [6, 7]. MUBs correspond to measurement bases that are most 'incompatible', as quantified by uncertainty relations [8] and other incompatibility measures [9, 10], and, the security of quantum cryptographic tasks relies on this property of MUBs. In particular, protocols based on higher-dimensional quantum systems with larger numbers of unbiased basis sets can have certain advantages over those based on qubits [11, 12]. It is therefore important for cryptographic applications to identify sets of MUBs in higher-dimensional systems that satisfy strong uncertainty relations.

The maximum number of MUBs that can exist in a d-dimensional Hilbert space is $d + 1$ and explicit constructions of such complete sets are known when d is a prime power [2, 13, 14]. One such construction is based on forming *mutually disjoint maximal commuting classes* from a unitary operator basis. Specifically, consider a set $\mathcal{U}$ of d^2 unitary operators that forms a basis for the space of $d \times d$ complex matrices. If there exist subsets $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L | \mathcal{C}_j \subset \mathcal{U} \setminus \{\mathcal{I}\}\}$ of size $|\mathcal{C}_j| = d - 1$ such that, (a) the elements of $\mathcal{C}_j$ commute for all $1 \leq j \leq L$ and (b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$, then, it was shown in [13] that the common eigenbases of L such disjoint maximal commuting classes form a set of L mutually unbiased bases.

When the unitary basis is comprised of the generalized Pauli operators, this approach provides a construction of a complete set of $d+1$ MUBs in prime-power dimensions ($d = p^n$). In terms of the computational basis $\{|j\rangle, j = 1, \ldots, p\}$, the generalized Pauli operators $\mathcal{X}_p, \mathcal{Z}_p$ (also the generators of the Weyl-Hiesenberg group) in p-dimensions are given by

$$\mathcal{X}_p|j\rangle = |(j+1) mod\ p\rangle; \quad \mathcal{Z}_p|j\rangle = e^{i2\pi j/p}|j\rangle.$$

Now, let $\mathcal{U}_{p,n}$ be the set of unitaries in dimension $d = p^n$ that are generated as n-fold tensor products of products of $\mathcal{X}_p$ and $\mathcal{Z}_p$. Then, it was shown that the set $\mathcal{U}_{p,n}/\{\mathbb{I}\}$ can always be partitioned into such a set of $d + 1$ maximal commuting classes in $d = p^n$ dimensions, their common eigenbases forming a complete set of $d + 1$ MUBs [13].

However, in non-prime-power dimensions, the question of whether a complete set of MUBs exists remains unresolved. Related to the question of finding complete sets of MUBs is the important concept of *unextendible* sets of MUBs. A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is said to be **unextendible** if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to all the bases $\mathcal{B}_j, j = 1, \ldots, m$. Examples of such unextendible sets are known in the literature. In dimension $d = 6$, the three eigenbases of $\mathcal{X}_6, \mathcal{Z}_6$ and $\mathcal{X}_6\mathcal{Z}_6$ were shown to be an unextendible set of MUBs [15]. This has the important consequence that the eigenbases of Weyl-Hiesenberg generators will not lead to a complete set of 7 MUBs in $d = 6$. In fact, several distinct families of unextendible triplets of MUBs have been constructed in $d = 6$ [16–18]. Moving away from six dimensions, the set of three MUBs obtained in $d = 4$ using Mutually Orthogonal Latin Squares (MOLS) [19] is an example of an unextendible set of MUBs in prime-power dimensions [20].

More recently, a systematic construction of such smaller sets that are unextendible to a complete set was obtained for two- and three-qubit systems [21]. Specifically, it was shown that there exist smaller sets of $k = \frac{d}{2} + 1$ commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k\}$ in $d = 2^n$ that are *unextendible* in the following sense—no more maximal commuting classes can be formed out of the remaining n-qubit Pauli operators that are not contained in $\mathcal{C}_1 \cup \mathcal{C}_2 \ldots \cup \mathcal{C}_k$. The eigenbases of $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ thus constitute a **weakly unextendible** set of k MUBs which cannot be extended to a complete set of $d + 1$ MUBs using Pauli classes. While an explicit construction of such unextendible classes was provided for $d = 4, 8$, their existence was conjectured for $d = 2^n (n > 3)$. This conjecture has been further improved upon [22] using a correspondence between unextendible sets of MUBs and maximal partial spreads of the polar space formed by the n-qubit Pauli operators [23].

Here, we show the existence of weakly unextendible sets of MUBs in prime-squared dimensions $d = p^2$, where p is prime. Each basis is realized as the common eigenbasis of a maximal commuting class of tensor products of the generalized Pauli operators. While the existence of unextendible sets of classes in $d = p^2$ has been shown recently using the geometry of symplectic polar spaces [22], we provide an algebraic construction which makes it easier to visualize the corresponding bases. Our construction also brings to light an interesting connection between the existence of unextendible sets and the tightness of entropic lower bounds in these dimensions. In particular, we identify sets of $p + 1$ MUBs that saturate both a Shannon and a collision EUR in $d = p^2$. We merely state our results here and refer to the technical supplement [28] for further details and proofs.

First Result: [Unextendible sets of $p^2 - p + 2$ classes in $d = p^2$ for $p \geq 3$]
Given $\mathcal{U}_{p,2}$, the set of unitaries in $d = p^2$ generated by $\mathcal{X}_p$ and $\mathcal{Z}_p$, we provide an explicit construction of unextendible sets of $N(p) = p^2 - p + 2$ classes for $p \geq 3$. For the case of $p \geq 3$, our construction crucially relies on the following fact: there exist a set of $p+1$ classes that are a part of the complete set of $p^2 + 1$ classes out of which, exactly 2 more maximal commuting classes can be formed. Therefore, these two new classes along with the remaining $p^2 - p$ classes form an unextendible set of $N(p)$ classes.
Example in $p = 3$, $d = 9$: Consider the following four maximal commuting classes which are part of a complete set of ten classes – $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{10}\}$ – in $d = 3^2$:

$$\begin{aligned}
\mathcal{C}_1 &= \left\langle\, \mathcal{I}_3 \otimes \mathcal{X}_3\mathcal{Z}_3^2,\; \mathcal{X}_3\mathcal{Z}_3 \otimes \mathcal{I}_3 \,\right\rangle \\
\mathcal{C}_2 &= \left\langle\, \mathcal{Z}_3 \otimes \mathcal{X}_3\mathcal{Z}_3^2,\; \mathcal{X}_3 \otimes \mathcal{X}_3 \,\right\rangle \\
\mathcal{C}_5 &= \left\langle\, \mathcal{Z}_3 \otimes \mathcal{X}_3^2\mathcal{Z}_3,\; \mathcal{X}_3 \otimes \mathcal{X}_3^2 \,\right\rangle \\
\mathcal{C}_7 &= \left\langle\, \mathcal{I}_3 \otimes \mathcal{X}_3\mathcal{Z}_3,\; \mathcal{Z}_3 \otimes \mathcal{I}_3 \,\right\rangle
\end{aligned}$$

Note that we describe each class $\mathcal{C}_i$ in terms of their *generators* – the remaining operators in the class are simply realized as higher powers and products of these [29]. From the elements of

$\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$, we can form *exactly* two more classes:

$$\begin{aligned} \mathcal{C}_I &= \left\langle\, \mathcal{I} \otimes \mathcal{X}_3 \mathcal{Z}_3^2,\ \mathcal{Z}_3 \otimes \mathcal{X}_3 \mathcal{Z}_3^2 \,\right\rangle \\ \mathcal{C}_{II} &= \left\langle\, \mathcal{X}_3 \mathcal{Z}_3 \otimes \mathcal{I},\ \mathcal{X}_3 \mathcal{Z}_3 \otimes \mathcal{X}_3^2 \mathcal{Z}_3^2 \,\right\rangle \end{aligned}$$

$\mathcal{C}_I, \mathcal{C}_{II}$ contain exactly two elements from each of the four classes. Since no more maximal commuting classes can be formed using the elements of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$, the new classes $\mathcal{C}_I, \mathcal{C}_{II}$ along with the remaining classes $\{\mathcal{C}_5, \mathcal{C}_6, \ldots, \mathcal{C}_{10}\}$ constitute an unextendible set of 8 classes in $d = 3^2$ dimensions. The common eigenbasis of such an unextendible set of maximal commuting classes form a weakly unextendible set of 8 MUBs in a nine dimensional space.

Second Result: [Tightness of Shannon and H_2 EURs in $d = p^2$]
We further show that the existence of unextendible classes implies the tightness of an entropic uncertainty relation (EUR) for the Rényi entropy of order 2 - H_2 (also known as the collision entropy [30]) in prime-squared dimensions. In particular, given a set of $p + 1$ classes such that one more class $\mathcal{C}_I$ can be formed using the operators in the set, their common eigenbases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_{p+1}\}$ satisfy,

$$\frac{1}{p+1} \inf_{|\psi\rangle \in \mathbb{C}^{p^2}} \left[\sum_{i=1}^{p+1} H_2(\mathcal{B}_i || \psi\rangle) \right] = \log p = \frac{1}{2} \log d \ . \tag{1}$$

Equality is attained for common eigenstates of the new class $\mathcal{C}_I$. In other words, if the set of $p + 1$ classes corresponding to a given set of $p + 1$ MUBs are such that they give rise to an unextendible set of classes, then, the set of MUBs saturates the well known H_2 EUR [8]. The minimum uncertainty is attained for states that "look alike" with respect to each of the p+1 MUBs [24]. Our result generalizes an earlier observation that the H_2 EUR is tight for sets of 3 MUBs in $d = 4$ dimensions [21]. It further shows that the connection between the existence of unextendible classes and the tightness of this EUR which was earlier observed for only $d = 2^2$ holds for any prime-squared dimensions.

Finally, we also note that such a set of $p + 1$ classes – out of whose elements one more maximal commuting class can be formed – also leads to a tight Shannon EUR for the corresponding MUBs. In other words, $\mathcal{B}1, \mathcal{B}_2, \ldots, \mathcal{B}_{p+1}$ satisfy,

$$\frac{1}{p+1} \inf_{|\psi\rangle \in \mathbb{C}^{p^2}} \left[\sum_{i=1}^{p+1} H_2(\mathcal{B}_i || \psi\rangle) \right] = \log p = \frac{1}{2} \log d \ . \tag{2}$$

Equality is again achieved by common eigenstates of the new class formed by picking a pair of elements from each of the $p + 1$ classes. Note that this lower bound on the average Shannon entropy is in fact a *trivial* consequence of the Maassen-Uffink bound [25] for a pair of bases. It has been noted earlier that there exist sets of upto $p + 1$ MUBs in prime-squared dimensions constructed using the generalized Pauli operators that saturate the lower bound [26] in Eq (2). However, the question of identifying such a set of MUBs that satisfy a trivial Shannon EUR remains unresolved [8]. Here, we make some progress towards answering this question.
Applications: Two simple corollaries follow from the tightness of the Shannon EUR. The fact that the set of $p + 1$ MUBs satisfies a weak lower bound implies that such a set of MUBs cannot give a better locking result than just using a pair of MUBs [5]. On the other hand, such MUBs can be used to witness entanglement in $d \otimes d$ systems [27]. If a state $|\psi\rangle \in \mathbb{C}^{p^2} \otimes \mathbb{C}^{p^2}$ violates the Shannon EUR lower bound in Eq. (2), then, it must be entangled. However, this is not a necessary condition for the state to be entangled: there could exist entangled state that satisfy the EUR bound.
Conclusions: We show by explicit construction the existence of unextendible sets of $N(p) = p^2 - p + 2$ MUBs in prime squared ($d = p^2$) dimensions for $p \geq 3$. Our construction is based on grouping the generalized Pauli operators in these dimensions into sets of mutually disjoint, maximal commuting classes that are unextendible to a complete set of $(d + 1)$ classes. We further demonstrate a general connection between the

existence of unextendible sets and the tightness of an entropic uncertainty relation.

---

[1] I.D.Ivanovic, Journal of Physics A **14**, 3241 (1981).
[2] W. Wootters and B. Fields, Ann. Phys. **191** (1989).
[3] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, International journal of quantum information **8**, 535 (2010).
[4] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Physical Review A **86**, 022311 (2012).
[5] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Physical Review Letters **92**, 67902 (2004).
[6] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
[7] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).
[8] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).
[9] S. Bandyopadhyay and P. Mandayam, Physical Review A **87**, 042120 (2013).
[10] P. Mandayam and M. D. Srinivas, Physical Review A **89**, 062112 (2014).
[11] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters **88**, 127902 (2002).
[12] P. Mandayam and S. Wehner, Phys. Rev. A **83**, 022329 (2011).
[13] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[14] J. Lawrence, C. Brukner, and A. Zeilinger, Physical Review A **65**, 032320 (2002).
[15] M.Grassl, quant-ph/0406175v2 (2004).
[16] S. Brierley and S. Weigert, Physical Review A **79**, 052316 (2009).
[17] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner, Journal of Physics A: Math.Theor. **42**, 245305 (2009).
[18] D. McNulty and S. Weigert, Journal of Physics A: Math. Theor. **45**, 102001 (2012).
[19] P. Wocjan and T. Beth, Quantum Information and Computation **5**, 93 (2005).
[20] P. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan, Arxiv preprint quant-ph/0502024 (2005).
[21] P. Mandayam, S. Bandyopadhyay, M. Grassl, and W. K. Wootters, Quantum Information and Computing **14**, 0823 (2014).
[22] K. Thas, arXiv preprint arXiv:1407.2778 (2014).
[23] K. Thas, Europhysics Letters **86**, 6005 (2009).
[24] I. Amburg, R. Sharma, D. Sussman, and W. K. Wootters (2014), arXiv:1407.4074.
[25] H. Maassen and J. Uffink, Physical Review Letters **60** (1988).
[26] M. Ballester and S. Wehner, Physical Review A **75**, 022319 (2007).
[27] O. Gühne and M. Lewenstein, Physical Review A **70**, 022316 (2004).
[28] http://vishakhhegde.weebly.com/technical-documents.html
[29] For example, the class $\mathcal{C}_i = \langle U_i, V_i \rangle$ in $d = 3^2$ is comprised of the following set of $d - 1 = 8$ operators: $\mathcal{C}_i = \{U_i, V_i, U_i^2, V_i^2, U_iV_i, (U_i)^2V_i, U_iV_i^2, U_i^2V_i^2\}$
[30] The *collision entropy* H_2 of the distribution obtained by measuring state $|\psi\rangle$ in the measurement basis $\mathcal{B}_i = \{|b_i^{(j)}\rangle : j = 1, \ldots, d\}$ is defined as, $H_2(\mathcal{B}_i||\psi\rangle) = -\log \sum_{j=1}^{d} (|\langle b_i^{(j)}|\psi\rangle|^2)^2$.