Unextendible Mutually Unbiased Bases from Pauli Classes

Prabha Mandayam,[1] Somshubhro Bandyopadhyay,[2] Markus Grassl,[3] and William K. Wootters[4]

[1] *The Institute of Mathematical Sciences, Taramani, Chennai - 600113, India.*
[2] *Bose Institute, Bidhan Nagar, Kolkata - 700091, India.*
[3] *Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore.*
[4] *Williams College, Williamstown, MA - 01267, USA*

(Dated: June 16, 2013)

We provide a construction of sets of $d/2+1$ mutually unbiased bases (MUBs) in dimensions $d = 4, 8$ using maximal commuting classes of Pauli operators. We show that these incomplete sets cannot be extended further using the operators of the Pauli group. However, specific examples of sets of MUBs obtained using our construction are shown to be *strongly unextendible*; that is, there does not exist another vector that is unbiased with respect to the elements in the set. We conjecture the existence of such unextendible sets in higher dimensions $d = 2^n (n > 3)$ as well.

Furthermore, we prove an interesting connection between these unextendible sets and state-independent proofs of the Kochen-Specker Theorem for two-qubit systems. Our construction also leads to a proof of the tightness of a H_2 entropic uncertainty relation for any set of three MUBs constructed from Pauli classes in $d = 4$.

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 $|b_j\rangle \in \mathcal{B}$,

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

A set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is called a set mutually unbiased bases (MUBs) if every pair of bases in the set is mutually unbiased. Such bases play an important role in our understanding of complementarity in quantum mechanics and are central to quantum cryptographic tasks such as quantum key distribution [1] and two-party protocols in the noisy-storage model [2]. MUBs correspond to measurement bases that are most 'incompatible', as quantified by uncertainty relations [3], and the security of these cryptographic tasks relies on this property of MUBs. MUBs also form a minimal and optimal set of orthogonal measurements for quantum state tomography [4, 5].

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 [5–7]. However, in composite dimensions, whether a complete set of MUBs exists, still remains an open problem. 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 $\mathcal{B}_j, j = 1, \ldots, m$. While examples of such unextendible sets are known [8, 9], we provide a systematic construction of such unextendible sets of MUBs for systems of n-qubits.

Specifically, let $\mathcal{P}_n/\{\mathbb{I}\}$ denote the set of n-qubit Pauli operators in $d = 2^n$ dimensions, excluding the identity operator $\mathbb{I}$. Our construction involves forming a collection of *mutually disjoint maximal commuting classes*, that is, subsets $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L | \mathcal{C}_j \subset \mathcal{P}_n/\{\mathbb{I}\}\}$ 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 $j \neq k$. The common eigenbases of L such disjoint maximal commuting classes form a set of L mutually unbiased bases [6].

The set $\mathcal{P}_n/\{\mathbb{I}\}$ can always be partitioned into such a set of $d+1$ maximal commuting classes in $d = 2^n$ dimensions, their common eigenbases forming a complete set of $d+1$ MUBs [6, 7]. Here, we show that there exist smaller sets of $k < d+1$ 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 set of k MUBs which cannot be extended using joint eigenvectors of maximal sets of commuting Paulis. We call such sets **weakly unextendible**.

We also obtain examples of *strongly unextendible* sets of MUBs using our construction of unextendible classes in $d = 4, 8$, that is, there does not exist even a single vector unbiased with respect to the bases in these sets. For two-qubit systems, our construction of unextendible sets of maximal commuting Pauli classes enables us to prove the tightness of an entropic uncertainty relation. Finally, we also demonstrate an interesting connection between unextendible sets of classes and state-independent proofs of the Kochen-Specker Theorem [10, 11].

We merely summarize our results here, and refer to the arxiv preprint [12] for further details and proofs.

Result 1 (Weakly Unextendible Sets of 3 MUBs in $d = 4$)**.** *Given three Pauli classes $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ that belong to a complete set of classes in $d = 4$, there exists exactly one more maximal commuting class of Pauli operators $\mathcal{S}$ (distinct from $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$) that can be formed using the operators in $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$.*

The class $\mathcal{S}$ along with the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$ (in the complete set) form an unextendible set of Pauli classes, whose common eigenbases form a weakly unextendible set of three MUBs.

For example, the following set of three Pauli classes

$$\begin{aligned}\mathcal{C}_1 &= \{Y \otimes Y, I \otimes Y, Y \otimes I\},\\ \mathcal{C}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\},\\ \mathcal{C}_3 &= \{X \otimes I, I \otimes Z, X \otimes Z\},\end{aligned} \tag{2}$$

is an unextendible set obtained using our construction. Correspondingly, the common eigenbases of $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ form a set of *weakly unextendible* MUBs.

Result 2 (**Five Weakly Unextendible MUBs in** $d = 8$)**.** *Given five maximal commuting Pauli classes $\mathcal{C}_1, \ldots, \mathcal{C}_5$ that belong to a complete set of classes in dimension $d = 8$, there exists exactly one more maximal commuting class that can be constructed using the elements of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_5$. Denoting this new class as $\mathcal{S}$, $\{\mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_8, \mathcal{C}_9, \mathcal{S}\}$ is a set of five unextendible Pauli classes, the common eigenbases of which form a set of weakly unextendible MUBs in $d = 8$.*

In fact, we show that the number of MUBs in a weakly unextendible set is exactly *three* in $d = 4$ dimensions and $five$ in $d = 8$ dimensions; no more, no fewer. We also present examples of sets obtained from our construction, that are in fact strongly unextendible [12].

Properties of Unextendible Sets in $d = 4$**:** Our construction of unextendible sets of classes in dimensions where a complete set of such classes exist, offers new insight into the structure of MUBs in these dimensions. We now discuss potential applications of such smaller sets of MUBs for quantum foundations and for cryptographic tasks.

State-independent Proofs of the KS Theorem: Consider the set of three MUBs in $d = 4$ in (2). There exists an alternate partitioning of the nine operators that constitute the set, leading to another set of three commuting classes, namely,

$$\begin{aligned}\mathcal{C}'_1 &= \{Y \otimes Y, Z \otimes X, X \otimes Z\},\\ \mathcal{C}'_2 &= \{I \otimes Y, X \otimes Y, X \otimes I\},\\ \mathcal{C}'_3 &= \{Y \otimes I, Y \otimes Z, I \otimes Z\}.\end{aligned} \tag{3}$$

The new classes $\mathcal{C}'_i$ are formed by picking one commuting element each from each of $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$. Each of the 9 Pauli operators in (2) is a part of two maximal commuting classes – $\mathcal{C}_i$ and $\mathcal{C}'_i$. The partitions in (2) and (3) provide two separate *contexts* for each of these 9 Pauli operators, thus leading to a state-independent proof of the Kochen-Specker (KS) Theorem in $d = 4$ similar to the proof by Mermin [11].

We show here that the existence of two such contexts for the same set of nine operators is a property unique to unextendible sets of classes in $d = 4$. The existence of two such partitions of the same set of nine operators is not possible for an arbitrary triple of commuting classes that we may pick out of the complete set of five classes that exist in $d = 4$.

Result 3 (State-independent Proofs of the KS Theorem). *Given an unextendible set of three maximal commuting Pauli classes $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$, the nine operators that constitute these classes can be partitioned into a different set of three maximal commuting classes $\{\mathcal{C}'_1, \mathcal{C}'_2, \mathcal{C}'_3\}$ such that $\mathcal{C}'_i$ has one operator each from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$.*

Our construction thus provides a systematic way to construct Mermin-like proofs in $d = 4$ and could potentially lead to stronger tests of contextuality. In fact, combining such Mermin-like proofs has been shown to yield a stronger violation of non-contextuality [13, 14] than simply using Mermin's proof.

Tightness of H_2 EUR: MUBs correspond to measurement bases that are most "incompatible", where the degree of incompatibility is quantified by entropic uncertainty relations (EURs). Here we will focus on the *collision entropy* H_2 of the distribution obtained by measuring state $|\psi\rangle$ in the measurement basis $\mathcal{B}_i = \{|b_i^{(j)}\rangle, j = 1, \ldots, d\}$, defined as, $H_2(\mathcal{B}_i||\psi\rangle) = -\log\sum_{j=1}^{d}(|\langle b_i^{(j)}|\psi\rangle|^2)^2$.

For L MUBs in d dimensions, the collision entropy satisfies the following uncertainty relation [3]:

$$\frac{1}{L}\sum_{i=1}^{L} H_2(\mathcal{B}_i||\psi\rangle) \geq \log_2\left(\frac{L+d-1}{dL}\right). \tag{4}$$

However, it is not known if this EUR is tight in general. Here, we show that this uncertainty relation is in fact tight for any three MUBs in $d = 4$, whether they be (a) part of a complete set of MUBs, or (b) a set of weakly unextendible MUBs.

Result 4 (Tightness of H_2 Entropic Uncertainty Relation). *Given a set of three maximal commuting Pauli classes $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$ in dimension $d = 4$, let $\mathcal{S}$ be the maximal class constructed by picking one element from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$. Then, the common eigenstates of the operators in $\mathcal{S}$ saturate* (4)*, with $\mathcal{B}_i$ denoting the common eigenbasis of the operators in $\mathcal{C}_i$.*

Conclusions: We have explored the question of whether there exist smaller, unextendible sets of mutually unbiased bases in dimensions $d = 2^n$. We show by explicit construction the existence of sets of $d/2+1$ MUBs in dimensions $d = 4, 8$ from Pauli classes, that are unextendible using common eigenbases of operator classes from the Pauli group. Our construction is based on grouping the n-qubit Pauli operators into unextendible sets of $d/2 + 1$ maximal commuting classes. We show that specific examples of such unextendible Pauli classes in fact lead to strongly unextendible MUBs.

Since our construction relies on general properties of a complete set of Pauli classes which hold for any $d = 2^n$, we are led to conjecture the existence of such unextendible classes in higher dimensions ($n > 3$) as well. Since our construction essentially relies on partitioning a unitary operator basis into classes of commuting operators, it has the potential to be generalized to the case of prime-power dimensions.

In the case of two-qubit systems we prove that unextendible sets of Pauli classes lead to state-independent proofs of the Kochen-Specker Theorem. We also show that the tightness of the H_2 EUR for any set of three MUBs in $d = 4$ follows as an important consequence of our construction.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.

[2] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).

[3] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).

[4] I.D.Ivanovic, Journal of Physics A **14**, 3241 (1981).

[5] W. Wootters and B. Fields, Ann. Phys. **191** (1989).

[6] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[7] J. Lawrence, C. Brukner, and A. Zeilinger, Physical Review A **65**, 032320 (2002).

[8] M.Grassl, quant-ph/0406175v2 (2004).

[9] P. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan, Arxiv preprint quant-ph/0502024 (2005).

[10] S. Kochen and E. Specker, Journal of Mathematics and Mechanics **17**, 59 (1967).

[11] N. Mermin, Physical Review Letters **65**, 3373 (1990).

[12] P. Mandayam, S. Bandyopadhyay, M. Grassl, and W. K. Wootters, arXiv preprint arXiv:1302.3709 (2013), URL `http://arxiv.org/abs/1302.3709`.

[13] A. Cabello, Phys. Rev. A **82**, 032110 (2010).

[14] M. Kleinmann, O. Gühne, J. R. Portillo, J.-Å. Larsson, and A. Cabello, New Journal of Physics **13**, 113011 (2011).