A transform of complementary aspects with applications to entropic uncertainty relations

Prabha Mandayam* and Stephanie Wehner†
Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA

Niranjan Balachandran‡
Department of Mathematics, California Institute of Technology, Pasadena CA 91125, USA

(Dated: April 29, 2010)

Even though mutually unbiased bases and entropic uncertainty relations play an important role in quantum cryptographic protocols they remain ill understood. Here, we construct special sets of up to $2n+1$ mutually unbiased bases (MUBs) in dimension $d = 2^n$ which have particularly beautiful symmetry properties derived from the Clifford algebra. More precisely, we show that there exists a unitary transformation that cyclically permutes such bases. This unitary can be understood as a generalization of the Fourier transform, which exchanges two MUBs, to multiple complementary aspects. We proceed to prove a lower bound for min-entropic entropic uncertainty relations for any set of MUBs, and show that symmetry plays a central role in obtaining tight bounds. For example, we obtain for the first time a tight bound for four MUBs in dimension $d = 4$, which is attained by an eigenstate of our complementarity transform. Finally, we discuss the relation to other symmetries obtained by transformations in discrete phase space, and note that the extrema of discrete Wigner functions are directly related to min-entropic uncertainty relations for MUBs.

I. INTRODUCTION

One of the central ideas of quantum mechanics is the uncertainty principle which was first proposed by Heisenberg [1] for two conjugate observables. Indeed, it forms one of the most significant examples showing that quantum mechanics does differ fundamentally from the classical world. Uncertainty relations today are probably best known in the form given by Robertson [2], who extended Heisenberg's result to two arbitrary observables A and B. Robertson's relation states that if we prepare many copies of the state $|\psi\rangle$, and measure each copy individually using either A or B, we have

$$\Delta A \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle| \tag{1}$$

where $\Delta X = \sqrt{\langle\psi|X^2|\psi\rangle - \langle\psi|X|\psi\rangle^2}$ for $X \in \{A, B\}$ is the standard deviation resulting from measuring $|\psi\rangle$ with observable X. The essence of (1) is that quantum mechanics does not allow us to simultaneously specify definite outcomes for two non-commuting observables when measuring the same state. The largest possible lower bound in Robertson's inequality (1) is 1, which happens if and only if A and B are related by a Fourier transform, that is, they are conjugate observables.

Of particular importance to quantum cryptography is the case where A and B correspond to measurements in two different orthonormal bases $\mathcal{A} = \{|a\rangle\}_a$ and $\mathcal{B} = \{|b\rangle\}_b$ in dimension d. If $\mathcal{A}$ and $\mathcal{B}$ are related by the Fourier transform, for all basis vectors $|a\rangle$ of basis $\mathcal{A}$ and all vectors $|b\rangle$ of basis $\mathcal{B}$,

$$|\langle a|b\rangle|^2 = \frac{1}{d}\ . \tag{2}$$

Any two bases satisfying this property are called *mutually unbiased bases*, or *complimentary aspects*, and in turn the unitary that exchanges two mutually unbiased bases can be understood as a Fourier transform. In the light of Robertson's uncertainty relation (1), it seems that bases which are related by the Fourier transform should play a special role in our understanding of quantum mechanics, in the sense that they are the measurements which are most "incompatible".

However, nature typically allows us to perform more than two measurements on any given system, leading to the natural question of how we can determine "incompatibility" between multiple measurements. Clearly, due to its use of the commutator relation, the lower bound of (1) most directly relates to the case of *two* measurements. Is there a natural way of quantifying uncertainty for multiple measurements? And if so, what measurements might be most "incompatible"?

A. Entropic uncertainty relations

A natural measure that captures the relations among the probability distributions over the outcomes for each observable is the entropy of such distributions. This prompted Hirschmann to propose the first entropic uncertainty relation for position and momentum observables [3]. This relation was later improved by [4, 5], where [5] show that Heisenberg's uncertainty relation (1) is in fact implied by this entropic uncertainty relation. Hence, using entropic quantities provides us with a much

*prabhamd@caltech.edu
†wehner@caltech.edu
‡nbalacha@caltech.edu

more general way of quantifying uncertainty. Indeed, it was realized by Deutsch [6] that other means of quantifying "uncertainty" are also desirable for another reason: Note that the lower bound in (1) is trivial when $|\psi\rangle$ happens to give zero expectation on $[A, B]$. Hence, it would be useful to have a way of measuring "incompatibility" which depends only on the measurements A and B and not on the state. Deutsch [6] himself showed that

$$\frac{1}{2}\left(H_\infty(\mathcal{A}||\psi\rangle) + H_\infty(\mathcal{B}||\psi\rangle)\right) \geq -\log\left(\frac{1+c(\mathcal{A},\mathcal{B})}{2}\right) \tag{3}$$

where $c(\mathcal{A},\mathcal{B}) := \max\{|\langle a|b\rangle| \mid |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}\}$, and

$$H_\infty(\mathcal{A}||\psi\rangle) = -\log \max_a |\langle a|\psi\rangle|^2 \tag{4}$$

is the min-entropy arising from measuring the pure state $|\psi\rangle$ using the basis $\mathcal{A}$ (see Section III A for more information on the entropic quantities we use). If $\mathcal{A}$ and $\mathcal{B}$ are related by a Fourier transform, then the r.h.s. of (3) becomes $-\log(1/2 + 1/(2\sqrt{d}))$, where the minimum is achieved by a state that is invariant under the Fourier transform. Since the Shannon entropy obeys $H(\cdot) \geq H_\infty(\cdot)$, Deutsch's bound also holds for the Shannon entropy. Better lower bounds have since been obtained for the Shannon entropy by Maassen and Uffink [7] following a conjecture of Kraus [8]. Their uncertainty relations are again strongest (in the sense that the lower bound is largest) when the bases $\mathcal{A}$ and $\mathcal{B}$ are conjugate, that is, the two bases are related by a Fourier transform. Apart from their role in understanding the foundations of quantum mechanics, these uncertainty relations play a central role in cryptography in the noisy-storage model [9–13], quantum key distribution [14, 15], information locking [16], and the question of separability [17].

Here, we are concerned with measurements in multiple bases $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$. Next to their foundational significance, such relations have practical interest in noisy-storage cryptography [11] where they may enable us to prove security for a larger class quantum memories. Entropic uncertainty relations provide a natural way of quantifying "incompatibility" of more than two measurements by lower bounding

$$\frac{1}{L}\sum_{j=0}^{L-1} H(\mathcal{B}_j||\psi\rangle) \geq c_L \ , \tag{5}$$

for all states $|\psi\rangle$. We thereby call a state $|\psi\rangle$ that minimizes the average sum of entropies a *maximally certain state*. When H is the Shannon entropy, the largest bound we can thereby hope to obtain for any choice of bases is

$$c_L = \frac{L-1}{L}\ \log d \ , \tag{6}$$

since choosing $|\psi\rangle$ to be an element of one of the bases yields zero entropy when we subsequently measure in the same basis. If (6) is indeed a lower bound to (5), we will call the measurements *maximally incompatible with respect to the Shannon entropy*. Note that this can only happen if $|\psi\rangle$ gives us full entropy [45] when measured in any other basis, that is, the bases are all mutually unbiased.

Curiously, however, it was shown that whereas being mutually unbiased is necessary, it is not a sufficient condition to obtain maximally strong uncertainty relations for the Shannon entropy [18]. In particular, there do exist large sets of up to $\sqrt{d}$ mutually unbiased bases in square dimensions for which we do obtain very weak uncertainty relations [18]. Recently, Ambainis [19] has shown that for any three bases from the "standard" mutually unbiased bases construction [20, 21] in prime dimension, the lower bound cannot exceed $\left(\frac{1}{2} + o(1)\right)\log d$, for large dimensions. For dimensions of the form $4k+3$ and $8k+5$ no further assumption is needed, but the proof assumes the Generalized Riemann Hypothesis for dimensions of the form $8k+1$. Furthermore, for any $0 \leq \epsilon \leq 1/2$, there always exist $k = d^\epsilon$ of these bases such that the lower bound cannot be larger than $\left(\frac{1}{2} + \epsilon + o(1)\right)\log d$. Only if we use the maximal set of $d+1$ mutually unbiased bases that we can find for any given prime power dimension, do we obtain quite strong uncertainty relations [22, 23].

At present, we merely know that there do exist arbitrarily large sets of two outcome measurements that do give us maximally strong uncertainty relations [24], and that in larger dimensions selecting a large amount of bases at random does provide us with strong relations [25] (for a survey see [26]). Indeed, it remains an intriguing open question as to whether there even exist three measurements with three outcomes in dimension $d > 2$ that are maximally incompatible with respect to the Shannon entropy.

B. Mutually unbiased bases

In the light of these questions, it is therefore natural to study the structure of mutually unbiased bases(MUBs) to see whether we can identify additional properties which are sufficient for obtaining strong uncertainty relations. In [27], Wootters and Sussman made the interesting observation that for the maximal set of $d+1$ mutually unbiased bases coming from such constructions as [20, 21] in dimension $d = 2^n$, the lower bound of the entropic uncertainty relation in terms of the collision entropy given in [18] is tight, and the minimum is attained by a state that is invariant under a unitary that cyclically permutes the set of all $d+1$ MUBs. A similar unitary was noted to exist by Chau [28]. Wootters and Sussman thereby derive their transformation from phase space arguments. Their unitary can in fact easily be generalized to cyclically permute L bases, whenever L divides $d+1$ (see Section III B 2). The results in [27] have recently been generalized by Appleby [29], who shows that in prime power dimensions of the form $d = 1$ or $3 \mod 4$, there exists a unitary operation that cyclically permutes the

first and second halves of the full set of MUBs. This raises the pressing question of whether smaller sets of MUBs also exhibit such symmetries? And can we exploit such symmetries to obtain tight uncertainty relations? In particular, is the minimizing state always an invariant of such a transformation as observed for two bases in (3) ?

Main result We first show by an explicit construction that there exist sets of $2 \leq L \leq 2n+1$ mutually unbiased bases in dimension $d = 2^n$ with the property that there exists a unitary that cyclically permutes all bases in this set, whenever (a) L is prime, and (b) L divides n or $L = 2n + 1$. More specifically, we provide an explicit construction of MUBs $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ with $\mathcal{B}_j = \{|b^{(j)}\rangle\}_b$ and a unitary U such that

$$U|b^{(j)}\rangle\langle b^{(j)}|U^\dagger = |b^{(j+1 \mod L)}\rangle\langle b^{(j+1 \mod L)}| \quad \text{for all } |b^{(j)}\rangle \in \mathcal{B}_j \ . \tag{7}$$

Furthermore, in dimension $d = 4$, we actually find such a unitary for any set of L MUBs, where $2 \leq L \leq 5$. Our approach exploits properties of the Clifford algebra, which might yield new insights into the structure of MUBs. It is entirely distinct from the phase space approach which was used to construct such a unitary for the full set of $d+1$ MUBs [20]. Note that our construction gives at most $O(\log d)$ bases, but shows that there is indeed an additional symmetry which has previously gone unnoticed. For $L = 2$ bases, U is simply the Fourier transform, and it would be interesting to investigate general properties of our transformation and whether it has applications in other areas.

C. Min-entropic uncertainty relations

We then apply our transformation to the study of uncertainty relations in terms of the *min-entropy* (see (4)). Since $H(\cdot) \geq H_\infty(\cdot)$, this also provides us with bounds on uncertainty relations in terms of the Shannon entropy. Of course, many forms of entropy could be considered when it comes to quantifying uncertainty, and each has its merits. The min-entropy is of particular interest in cryptography, and is easily related to the well studied extrema of the discrete Wigner function as we will discuss in Section III B 2. In particular, it will be easy to see that the average min-entropy for the full set of $L = d+1$ MUBs can be bounded as

$$\frac{1}{d+1}\sum_{j=0}^{d} H_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[d \cdot \left(\max_\alpha W_\alpha^{\max} + 1\right)\right] \ , \tag{8}$$

where $W_\alpha^{\max}$ is the maximum value of the discrete Wigner function at the point α in discrete phase space. Symmetries thereby play an important role in determining $W_\alpha^{\max}$.

Second result We prove a simple min-entropic uncertainty relation for an arbitrary set of L mutually unbiased bases. For MUBs $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ we obtain

$$\frac{1}{L}\sum_{j=0}^{L-1} H_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right]. \tag{9}$$

For the case of 2 MUBs in dimension d, this bound is indeed the same as the bound in (3). For any small set of $2 < L < d$ MUBs, our bound is slightly stronger than previously obtained bounds [30]. We also prove the following alternate lower bound:

$$\frac{1}{L}\sum_{j=0}^{L-1} H_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\right], \tag{10}$$

which is stronger than (9) for the complete set of $L = d+1$ MUBs in dimension d. Clearly, when $L = d$, the two bounds are equivalent.

We further show that (9) is in fact tight for $L = 4$ MUBs in dimension $d = 4$ stemming from our construction, where the minimum is attained for an invariant state of the transformation U that cyclically permutes all 4 bases. Even though this is a somewhat restricted statement, it is the first time that a tight entropic uncertainty relation has been obtained for this case. The minimizing state thereby has an appealing symmetry property, just as for the case of $L = 2$ bases in (3) where the minimum is attained by a state that is invariant under the Fourier transform.

For the collision entropy H_2, Wootters [27] previously showed that the lower bound from [18] is attained by an invariant state when considering the full set of $d + 1$ MUBs. Here, however, we exhibit a tight uncertainty relation for these $L = 3$ bases in $d = 4$ for the collision entropy H_2 which has an entirely different structure and the minimum is not attained by an invariant state of our transformation. Nevertheless, we thus have for the first time a *tight* entropic uncertainty relation for *all* possible MUBs in a dimension larger than the trivial case of $d = 2$ where the Bloch sphere representation makes the problem easily accessible. In $d = 4$, we have a tight relation for H_∞ for $L = 2, 4$, and tight relations for H_2 for $L = 3, 5$.

However, our result indicates that due to the different properties of the minimizing state for different numbers of bases, the problem may be even more daunting than previously imagined. Yet, our work shows that in each case the minimizing state is by no means arbitrary. It has a well defined (albeit different) structure in each of the cases.

Third result For some sets of MUBs we do obtain for the first time, significant insight into the structure of the maximally certain states. In particular, we note in Section III B 1 that for L mutually unbiased bases that the state that minimizes the min-entropic uncertainty relations is an invariant of a certain unitary whenever L divides $d + 1$ for $d = 2^n$.

II. SYMMETRIC MUBS

Before explaining our construction of mutually unbiased bases for which there exists a unitary that cyclically permutes them, let us define the notions of MUBs more formally and recall some known facts. Let $\mathcal{B}_1 = \{|0^{(1)}\rangle, \ldots, |d-1^{(1)}\rangle\}$ and $\mathcal{B}_2 = \{|0^{(2)}\rangle, \ldots, |d-1^{(2)}\rangle\}$ be two orthonormal bases in $\mathbb{C}^d$. They are said to be *mutually unbiased* if $|\langle a^{(1)}|b^{(2)}\rangle| = 1/\sqrt{d}$, for all $a, b \in \{0, \ldots, d-1\}$. A set $\{\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}\}$ of orthonormal bases in $\mathbb{C}^d$ is called a *set of mutually unbiased bases* if each pair of bases is mutually unbiased. For example, the well-known computational and Hadamard basis are mutually unbiased. We use $N(d)$ to denote the maximal number of MUBs in dimension d. In any dimension d, we have that $N(d) \leq d+1$ [21]. If $d = p^k$ is a prime power, we have that $N(d) = d+1$ and explicit constructions are known [20, 21]. Other constructions are known that give less than $d+1$ MUBs in other dimensions [31–34]. However, it is still an open problem whether there exists a set of 7 (or even 4!) MUBs in dimension $d = 6$.

A. Clifford algebra

Our construction of mutually unbiased bases makes essential use of the techniques developed in [21], together with properties of the Clifford algebra. The Clifford algebra is the associative algebra generated by operators $\Gamma_0, \ldots, \Gamma_{2n-1}$ satisfying $\{\Gamma_i, \Gamma_j\} = 0$ for $i \neq j$ and $\Gamma_i^2 = \mathbb{I}$. It has a unique representation by Hermitian matrices on n qubits (up to unitary equivalence) that can be obtained via the famous Jordan-Wigner transformation [35]:

$$\Gamma_{2j+1} = Y^{\otimes(j-1)} \otimes Z \otimes \mathbb{I}^{\otimes(n-j)}, \tag{11}$$

$$\Gamma_{2j} = Y^{\otimes(j-1)} \otimes X \otimes \mathbb{I}^{\otimes(n-j)}, \tag{12}$$

for $j = 0, \ldots, n-1$, where we use X, Y and Z to denote the Pauli matrices. Furthermore, we let

$$\Gamma_{2n} := i\Gamma_0 \ldots \Gamma_{2n-1} \ . \tag{13}$$

Note that in dimension $d = 2$ these are just the familiar Pauli matrices, $\Gamma_0 = X$, $\Gamma_1 = Z$ and $\Gamma_2 = Y$.

Of particular importance to us will be that we can view the operators $\Gamma_0, \ldots, \Gamma_{2n-1}$, as $2n$ orthogonal vectors forming a basis for $\mathbb{R}^{2n}$. In particular, for any orthonormal transformation $T \in \mathrm{O}(2n)$ which applied to the vector $v = (v^{(0)}, \ldots, v^{(2n-1)}) \in \mathbb{R}^{2n}$ gives $\tilde{v} = (\tilde{v}^{(1)}, \ldots, \tilde{v}^{(2n-1)}) = T(v)$, there exists a unitary $U(T)$ such that

$$U(T) \left(\sum_j v_j \Gamma_j \right) U(T)^\dagger = \sum_j \tilde{v}_j \Gamma_j \ . \tag{14}$$

The orthonormal transformation that is particularly interesting to us here is the one that cyclically permutes the basis vectors. By the above we can find a corresponding unitary $U = U(T)$ which cyclically permutes the basis vectors $\Gamma_0, \Gamma_2, \ldots, \Gamma_{L-1}$. An explicit construction can be found in the appendix. This symmetry can be extended to $\mathrm{SO}(2n+1)$, see e.g. [24]. It will also be useful that the set of d^2 operators

$$\mathcal{S} = \{\mathbb{I}, \Gamma_j, i\Gamma_i\Gamma_j, \Gamma_i\Gamma_j\Gamma_k, \ldots, i\Gamma_1 \ldots \Gamma_{2n}\} \tag{15}$$

forms an orthogonal basis [46] for $d \times d$ Hermitian matrices in $d = 2^n$ [36].

B. Construction

To construct mutually unbiased bases, we follow the procedure outlined in [21], but now applied to a subset of the operators in $\mathcal{S} \setminus \{\mathbb{I}\}$. That is, we will group operators into classes of commuting operators, i.e., sets $\{\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{L-1} \mid \mathcal{C}_j \subset \mathcal{S} \setminus \{\mathbb{I}\}\}$ of size $|\mathcal{C}_j| = d-1$ such that

(i) the elements of $\mathcal{C}_j$ commute for all $0 \leq j \leq L-1$,

(ii) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.

It has been shown in [21] that the common eigenbases of such classes form a set of L MUBs.

First of all, note that no class can contain two generators Γ_j and Γ_k since they do not commute. When forming the classes we hence ensure that each one contains exactly one generator Γ_j, which clearly limits us to constructing at most $2n+1$ such classes. The difficulty in obtaining a partitioning that is suitable for our purpose is to ensure that the unitary U that cyclically permutes the generators $\Gamma_0, \ldots, \Gamma_{L-1}$ also permutes the corresponding bases by permuting products of operators appropriately. We show in the appendix that our general construction achieves the following:

Theorem II.1. *Suppose that $2 \leq L \leq 2n+1$ is prime, and either L divides n or $L = 2n+1$. Then in dimension $d = 2^n$, there exist L mutually unbiased bases $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ for which there exists a unitary U that cyclically permutes them*

$$U\mathcal{B}_j = \mathcal{B}_{j+1 \mod L} \ . \tag{16}$$

C. Examples

Let us consider two simple examples of such classes in dimension $d = 4$. These are not obtained from our general construction, but nevertheless provide us with the necessary intuition. For $L = 3$ MUBs the classes are given by

$$\begin{aligned} \mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_3\Gamma_2\} \\ \mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\ \mathcal{C}_2 &= \{\Gamma_2, i\Gamma_0\Gamma_4, i\Gamma_3\Gamma_1\} \end{aligned} \tag{17}$$

It is easy to see that the unitary U that achieves the transformation $\Gamma_0 \to \Gamma_1 \to \Gamma_2 \to \Gamma_0$, but leaves Γ_3 and Γ_4 invariant, cyclically permutes the bases given above. For the collision entropy H_2 the minimum is attained for an eigenstate of the *commuting* operators Γ_0, $i\Gamma_2\Gamma_4$ and $i\Gamma_3\Gamma_1$. This minimizing state also shows that the general bound for H_2 (see e.g. [26]) can be *tight*.

For $L = 4$ MUBs we obtain the classes

$$\begin{aligned} \mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_2\Gamma_3\} \\ \mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\ \mathcal{C}_2 &= \{\Gamma_2, i\Gamma_3\Gamma_4, i\Gamma_0\Gamma_1\} \\ \mathcal{C}_3 &= \{\Gamma_3, i\Gamma_0\Gamma_4, i\Gamma_1\Gamma_2\} \end{aligned} \tag{18}$$

It is easy to see that the unitary U that achieves the transformation $\Gamma_0 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to \Gamma_0$, but leaves Γ_4 invariant, cyclically permutes the bases given above. For $L = 4$ classes the minimum in the entropic uncertainty relation for H_∞ is attained for a state that is invariant under the transformation U. However, we also know that for $L = 4$ or $L = 8$ classes in dimension $d = 8$ no partitioning of operators is possible that satisfies our requirements. Thus, for what values of L and d such a unitary can be found, remains an interesting open question.

III. UNCERTAINTY RELATIONS

We now investigate the relationship between the observed symmetries and entropic uncertainty relations.

A. Entropic quantities

Before comparing different uncertainty relations, we first provide a short introduction to all the entropic quantities we will use. The expert reader may safely skip this section. In general, we can consider the *Rényi entropy* [37] of order α of the distribution obtained by measuring a state $|\psi\rangle$ in the basis $\mathcal{B} = \{|b\rangle\}_b$ which is given by

$$H_\alpha(\mathcal{B}||\psi\rangle) = \frac{1}{1-\alpha} \log \left[\left(\sum_{b\in\mathcal{B}} (|\langle b|\psi\rangle|^2)^\alpha \right)^{\frac{1}{\alpha-1}} \right]. \tag{19}$$

Indeed, the Shannon entropy forms a special case of the Rényi entropy by taking the limit $\alpha \to 1$, i.e., $H_1(\cdot) = H(\cdot)$, where we omit the subscript. Of particular importance is the *min-entropy*, for $\alpha \to \infty$:

$$H_\infty(\mathcal{B}||\psi\rangle) = -\log \left(\max_{b\in\mathcal{B}} |\langle b|\psi\rangle|^2 \right) , \tag{20}$$

and the *collision entropy*

$$H_2(\mathcal{B}||\psi\rangle) = -\log \sum_{b\in\mathcal{A}} (|\langle b|\psi\rangle|^2)^2 . \tag{21}$$

We have

$$\log d \geq H(\cdot) \geq H_2(\cdot) \geq H_\infty(\cdot) \geq 0 , \tag{22}$$

and hence uncertainty relations for H_α also provide us with a bound on uncertainty relations for H_β whenever $\alpha \geq \beta$.

Note that intuitively, the min-entropy is determined by the highest peak in the distribution and most closely captures the notion of "guessing". To see why it is a more useful quantity in cryptography than the Shannon entropy, consider the following example distribution P_X: Let $\mathcal{X} = \{0,1\}^n$ and let $x_0 = 0,\ldots,0$ be the all 0 string. Suppose that $P_X(x_0) = 1/2 + 1/(2^{n+1})$ and $P_X(x) = 1/(2^{n+1})$ for $x \neq x_0$, i.e., with probability $1/2$ we choose x_0 and with probability $1/2$ we choose one string uniformly at random. Then $H(X) \approx n/2$, whereas $H_\infty(X) \approx 1$! If x would correspond to an encryption key used to encrypt an n bit message, we would certainly not talk about security if we can guess the key with probability at least $1/2$! Yet, the Shannon entropy is quite high.

B. Min-entropy and symmetry

Apart from its cryptographic applications, min-entropic uncertainty relations are appealing since the problem of determining tight uncertainty relations can be simplified considerably in the presence of symmetries. Furthermore, these relations bear an interesting relation to the extrema of the discrete Wigner function. First of all, note that for the min-entropy we have by Jensen's inequality that

$$\frac{1}{L} \sum_{j=0}^{L-1} H_\infty(\mathcal{B}_j|\rho) \tag{23}$$

$$\geq -\log \frac{1}{L} \sum_{j=0}^{L-1} \max_{b^{(j)}} \mathrm{tr}(\rho|b^{(j)}\rangle\langle b^{(j)}|) \tag{24}$$

where the inequality becomes equality if all terms $\mathrm{tr}(\rho|b^{(j)}\rangle\langle b^{(j)}|)$ are the same. For $\vec{b} = (b^{(0)},\ldots,b^{(L-1)}) \in \{0,\ldots,d-1\}^{\times L}$, define

$$P_{\vec{b}} := \sum_{b^{(j)}} |b^{(j)}\rangle\langle b^{(j)}| . \tag{25}$$

Note that determining a tight lower bound to (24) is thus equivalent to determining

$$\max_{\vec{b}} \max_{\rho} \mathrm{tr}(\rho P_{\vec{b}}) . \tag{26}$$

Clearly, any ζ such that

$$P_{\vec{b}} \leq \zeta \mathbb{I} \text{ for all } \vec{b} \tag{27}$$

thus gives us a lower bound for (23). For any set of bases, this makes the problem of finding a bound more

approachable as it reduces the problem to finding the largest eigenvalue for any operator $P_{\vec{b}}$. In particular, it can be phrased as a semidefinite program where we minimize ζ such that (27) holds for all $\vec{b}$.

1. Symmetries

It is now easy to see why symmetries simplify our goal of determining tight uncertainty relations.

Lemma III.1. *Suppose that for every $\vec{b} \in \{0,\dots,d-1\}$ there exists a unitary $U_{\vec{b}}$ such that $U_{\vec{b}}|b^{(j)}\rangle = |b^{(j+1 \mod L)}\rangle$. Then there exists a $\vec{b'}$ such that the minimum in (23) is attained for a state ρ that is invariant under $U_{\vec{b'}}$.*

Proof. First of all, note that

$$\frac{1}{L}\sum_{j=0}^{L-1}(U_{\vec{b}}^j)P_{\vec{b}}(U_{\vec{b}}^j)^\dagger = P_{\vec{b}} \ , \tag{28}$$

and hence also for $\rho_{\mathrm{sym}} = (1/L)\sum_j (U_{\vec{b}}^j)^\dagger \rho (U_{\vec{b}}^j)$

$$\mathrm{tr}(\rho_{\mathrm{sym}}P_{\vec{b}}) = \mathrm{tr}(\rho P_{\vec{b}}) \ . \tag{29}$$

In particular, this holds for the state $\rho = |\psi\rangle\langle\psi|$ corresponding to the eigenvector $|\psi\rangle$ with the largest eigenvalue of $P_{\vec{b'}}$. When looking for the minimizing state on the r.h.s of (23) we can thus restrict ourselves to states which are invariant under $U_{\vec{b'}}^j$. Note that in this case, we furthermore have that

$$\mathrm{tr}(\rho_{\mathrm{sym}}|b^{(j)}\rangle\langle b^{(j)}|) = \frac{1}{L}\,\mathrm{tr}(\rho P_{\vec{b}}) \ , \tag{30}$$

meaning that the inequality (23) is tight in case of such a symmetry which is our claim. □

The question of course remains, whether such unitaries do exist in general. Wootters and Sussman [20] have shown that there exists a unitary U that cyclically permutes the set of all $d+1$ MUBs for $d = 2^n$ by constructing a unitary that corresponds to a rotation around the origin in phase space. Clearly, by considering the unitary U^k one can trivially adapt their construction to obtain a unitary that cyclically permutes L MUBs whenever $L \cdot k = d+1$. By first translating any point in the phase space to the origin, then applying the transformation U^k and finally translating the origin back to the original point, one can obtain the desired unitaries $U_{\vec{b}}$ that enable us to find tight bounds for the min-entropic uncertainty relations. This is the first time we gain significant insight into the structure of the states that minimize (23).

Note that our construction only gives unitaries $U_{\vec{b}}$ for $\vec{b} = (c,\dots,c)$ for any $c \in \{0,\dots,d-1\}$. This means that our complementarity transform U, leads to tight bounds only if the largest eigenvalue of any $P_{\vec{b}}$ happens to occur for a $\vec{b}$ of this form. This is for example the case for $L = 4$ in $d = 4$, where we do not obtain a unitary from the phase space approach of [20].

2. Discrete Wigner function

To see how finding a lower bound for min-entropic uncertainty relations for $d+1$ MUBs relates to finding the extrema of the discrete Wigner function, let us first recall the properties of the discrete Wigner function. The discrete phase space is a two-dimensional vector space over a finite field $\mathbb{F}_d$, where here we focus on the case of $d = 2^n$. For every state ρ, we can associate a function W_α with every point α in the discrete phase space, known as the discrete Wigner function. For completeness, we provide a very short summary on how to determine W_α; a detailed account can be found in [38]. First of all, note that the d^2 points of the discrete phase space can be parititioned into d parallel lines each of which contains d points. Any such partition is called a *striation*, and it is known that $d+1$ such striations can be found [38]. One may now define the discrete Wigner function by relating each striation to one of the $d+1$ possible mutually unbiased basis [38]: Let $\lambda_{b,j}$ denote the b-th line in the striation j. With each such line, we associate a projector

$$Q(\lambda_{b,j}) = |b^{(j)}\rangle\langle b^{(j)}| \ , \tag{31}$$

onto the b-th element of the basis $\mathcal{B}_j$, in a specific order so as to satisfy certain symmetry constraints [38]. Defining the phase-space point operator

$$A_\alpha := \sum_{\substack{\lambda_{b,j} \\ \alpha \subset \lambda_{b,j}}} Q(\lambda_{b,j}) - \mathbb{I} \ , \tag{32}$$

one can now define the discrete Wigner function as

$$W_\alpha := \frac{1}{d}\,\mathrm{tr}(A_\alpha \rho) \ . \tag{33}$$

The *extrema of the discrete Wigner function* are defined as the minimum and maximum of (33) over quantum states ρ.

Note that when considering $L = d+1$ mutually unbiased bases, each point α in the discrete phase space can be contained in exactly one line from each basis, as all lines in a striation, i.e., one basis are parallel. Hence, there is a one-to-one correspondence between points α in discrete phase space and vectors $\vec{b} \in \{0,\dots,d-1\}^{\times d+1}$. In terms of the phase space operator this means that $A_\alpha + \mathbb{I} = P_{\vec{b}}$ Note that the maximum of the discrete Wigner function

$$W_\alpha^{\max} = \max_\rho \frac{1}{d}\,\mathrm{tr}(A_\alpha \rho) \ , \tag{34}$$

is simply the largest eigenvalue of A_α (or $P_{\vec{b}} - \mathbb{I}$) up to a factor of $1/d$. We thus have that

$$\zeta := d \cdot \left[\max_\alpha W_\alpha^{\max} + 1\right] \ , \tag{35}$$

satisfies $P_{\vec{b}} \leq \zeta \mathbb{I}$ and the maximum of the discrete Wigner function provides a lower bound to the min-entropic uncertainty relations as given in (8). The extrema $W_\alpha^{\max}$ were evaluated numerically in [39] for small d. Note, however, that as noted in Section III B 1, one may use symmetries to solve the problem of determining $W_\alpha^{\max}$ directly.

C. A simple bound

As mentioned in Section III B, the problem of finding a lower bound for the average min-entropy reduces to the problem of finding the maximum eigenvalue of the operator $P_{\vec{b}}$ defined in (25). In the appendix, we use a result due to Schaffner [30] obtained using the techniques of Kittaneh [40], to show that for any set of L mutually unbiased bases in dimension d, the maximum eigenvalue of $P_{\vec{b}}$ is bounded by

$$P_{\vec{b}} \leq \frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\mathbb{I}, \text{ for all } \vec{b}. \tag{36}$$

Using this, we obtain the following simple bound for the average min-entropy in the appendix

Lemma III.2. *Let $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ be a set of mutually unbiased bases in dimension $d = 2^n$. Then*

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right] . \tag{37}$$

For the case of $L = 2$ MUBs in dimension d, our bound exactly matches the well known result of Deutsch (see (3)). For $L > 2$, the only other known lower bound for the average min-entropy is the one obtained in [30], where it is shown that for a set of $L < \sqrt{d}$ MUBs in dimension $d = 2^n$, the following holds:

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}} \max_{0\leq i<j\leq L-1} \sqrt{|X^i||X^j|}\right)\right] \tag{38}$$

where $|X^i|$ denotes the Hamming weight of the n-bit string $X^i \in \{0,1\}^n$. Since

$$\max_{0\leq i<j\leq L-1} \sqrt{|X^i||Y^j|} \geq 1, \tag{39}$$

our bound in (37) is clearly tighter than (38). The reason we obtain this slight improvement over [30] is that we reduce the problem directly to an eigenvalue problem without going through other techniques as in [30].

Using an alternate approach involving a Bloch sphere like representation of the basis vectors $|b^{(j)}\rangle$, we show that the maximum eigenvalue of $P_{\vec{b}}$ can be bound differently, as follows:

$$P_{\vec{b}} \leq \frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\mathbb{I}, \text{ for all } \vec{b}. \tag{40}$$

As we show in the appendix, this implies

Lemma III.3. *Let $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ be a set of mutually unbiased bases in dimension $d = 2^n$. Then*

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\right] . \tag{41}$$

Notice that this alternate bound on the min-entropy is stronger than (37) when $L > d$. In particular, for the complete set of $d+1$ MUBs in dimension d, this alternate bound in (41) is stronger than any previously known bounds. When $L = d$ the two bounds that we derive are indeed equivalent.

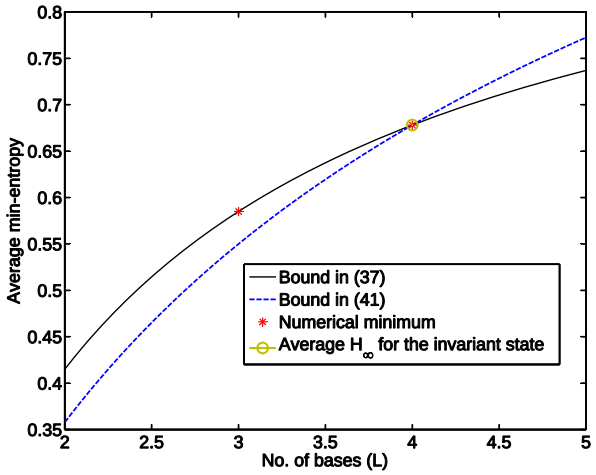

FIG. 1: Average min-entropy for different sets of MUBs in dimension $d = 4$.
The crosses denote numerically computed minima of the average min-entropy for MUBs obtained using our construction. The bound in (37) is clearly tight for both $L = 3$ and $L = 4$ MUBs. The second analytical bound in (41) is stronger than (37) for $L = d + 1 = 5$ bases. The circle denotes the average min-entropy for the invariant states given in (43). For 4 MUBs in $d = 4$ the minimum of the average min-entropy is indeed attained by states invariant under U.

Finally, we provide an example of a set of MUBs where Lemma III.2 is tight. For the set of $L = 4$ MUBs in dimension $d = 4$ constructed from the classes given in (18), our bound

$$\frac{1}{4}\sum_{j=0}^{3} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{4}\left(1 + \frac{3}{2}\right)\right] \approx 0.678 , \tag{42}$$

is tight, and the minimum is indeed achieved by a state that is invariant under the unitary transform that cycles through the bases, as defined in (16). As noted in Section III B 1, in this case, the largest eigenvalue of $P_{\vec{b}}$ occurs for a $\vec{b}$ of the form $\vec{b} = (c, \ldots, c)$ for any

$c \in \{0, \ldots, 3\}$. The states that achieve the lower bound are in fact eigenvectors of U, which can be expressed in terms of the MUB basis vectors as follows,

$$|\psi_b\rangle = \frac{1}{2} \sum_{j=0}^{3} \exp(i\pi j/4) |b^{(j)}\rangle, \; b \in \{0, \ldots, 3\}. \qquad (43)$$

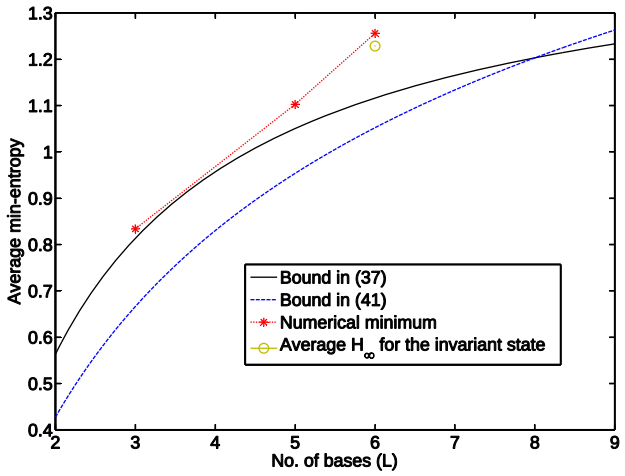

FIG. 2: Average min-entropy for different sets of MUBs in dimension $d = 8$.
The bound in (37) is close to tight for $L = 3$ MUBs in dimension $d = 8$. The second analytical bound in (41) is stronger than (37) for $L = d+1 = 9$ bases. The circle denotes the average min-entropy for invariant states constructed in dimension $d = 8$, similar to the states described in (43). For 6 MUBS in $d = 8$, the minimum of the average min-entropy is nearly attained by states invariant under U.

IV. CONCLUSIONS AND OPEN QUESTIONS

We have shown that there exist up to $2 \leq L \leq 2n + 1$ mutually unbiased bases in dimension $d = 2^n$ for which we can find a unitary that cyclically permutes these bases, whenever L is prime and L divides n or $L = 2n+1$. This unitary is found by exploiting symmetry properties of the Clifford algebra. Our approach is quite distinct from the phase space approaches that were previously used to show that there exists such a unitary for the set of all $d+1$ MUBs [20], or for two halves of the full sets of MUBs when $d = 1$ or 3 mod 4 [29]. Our unitary can be understood as a generalization of the Fourier transform, and it would be interesting to see whether it has other applications in quantum information.

It is an interesting open question to generalize our result to other dimensions, or to a different number of bases. In prime dimension, one could consider the generalized Clifford algebra [41]. Even though it does not have the full $SO(2n + 1)$ symmetry, it nevertheless exhibits enough symmetries to allow an exchange of generators. This stems from the way the (generalized) Clifford algebra is obtained [41, 42], which permits any transformation that preserves the p-norm for $p \geq 2$ in dimension p. Yet, this is only the first step of our construction. As for generalizing our result to any L bases in dimension $d = 2^n$, we note that it *is* indeed possible to find such classes even when L is not prime, as our example for $L = 4$ in dimension $d = 4$ shows. However, we also know that for $L = 8$ classes in dimension $d = 16$, no partitioning of operators can be found satisfying our requirements. It is an interesting open question as to when such a partitioning can be found in general.

Finally, we use our complementarity transform to obtain a tight uncertainty relation for the min-entropy for $L = 4$ bases in dimension $d = 4$. No tight relations are known for this case before. We also use a slight generalization of the unitary from [20] to show that when $d = 2^n$ and L divides $d + 1$, the minimizing state is an invariant of a certain unitary. This is the first time that significant insight has been obtained on the structure of the minimizing states for min-entropic uncertainty relations for mutually unbiased bases. It is an exciting open question to obtain tight relations in general, and understand the structure of the minimizing states.

Acknowledgments

We are grateful to David Gross for pointing us to the relevant literature for the discrete phase space construction. We also thank Lukasz Fidkowski and John Preskill for interesting discussions. PM and SW are supported by NSF grant PHY-0803371.

[1] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).
[2] H. Robertson, Physical Review **34**, 163 (1929).
[3] I. I. Hirschmann, American Journal of Mathematics **79** (1957).
[4] W. Beckner, Annals of Mathematics **102**, 159 (1975).
[5] I. Białynicki-Birula and J. Mycielski, Communications in Mathematical Physics **44** (1975).
[6] D. Deutsch, Physical Review Letters **50**, 631 (1983).
[7] H. Maassen and J. Uffink, Physical Review Letters **60** (1988).
[8] K. Kraus, Physical Review D **35**, 3070 (1987).
[9] S. Wehner, C. Schaffner, and B. M. Terhal, Physical Review Letters **100**, 220502 (2008).
[10] C. Schaffner, B. Terhal, and S. Wehner, Quantum Infor-

mation and Computation **9**, 0963 (2009).
[11] R. König, S. Wehner, and J. Wullschleger (2009), arXiv:0906.1030.
[12] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of 46th IEEE FOCS* (2005), pp. 449–458.
[13] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner (2007), proceedings of CRYPTO 2007.
[14] M. Koashi (2005), quant-ph/0505108.
[15] J. M. Renes and J.-C. Boileau, Physical Review A **78**, 032335 (2008).
[16] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Physical Review Letters **92** (2004).
[17] O. Guehne, Physical Review Letters **92**, 117903 (2004).
[18] M. Ballester and S. Wehner, Physical Review A **75**, 022319 (2007).
[19] A. Ambainis (2009), arXiv:0909.3720.
[20] W. Wootters and B. Fields, Ann. Phys. **191** (1989).
[21] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[22] J. Sanchez, Physics Letters A **173**, 233 (1993).
[23] I. D. Ivanovic, J. Phys. A: Math. Gen. **25**, 363 (1992).
[24] S. Wehner and A. Winter, Journal of Mathematical Physics **49**, 062105 (2008).
[25] P. Hayden, D. Leung, P. Shor, and A. Winter, Communications in Mathematical Physics **250**, 371 (2004).
[26] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010), special Issue on Quantum Information and Many-Body Theory.
[27] W. K. Wootters and D. M. Sussman (2007), arXiv:0704.1277.
[28] H. F. Chau, IEEE Transactions on Information Theory **51**, 1451 (2005).
[29] D. M. Appleby (2009), arXiv:0909.5233.
[30] C. Schaffner, Ph.D. thesis, University of Aarhus (2007).
[31] P. Wocjan and T. Beth, Quantum Information and Computation **5**, 93 (2005).
[32] G. Zauner, Ph.D. thesis, Universität Wien (1999).
[33] A. Klappenecker and M. Rötteler, in *International Conference on Finite Fields and Applications (Fq7)* (Springer, 2004), vol. 2948 of *Lecture Notes in Computer Science*, pp. 137–144.
[34] M. Grassl, in *Proceedings ERATO Conference on Quantum Information Science* (2004), pp. 60–61, quant-ph/0406175.
[35] P. Jordan and E. Wigner, Zeitschrift für Physik **47**, 631 (1928).
[36] K. Dietz, Journal of Physics A: Math. Gen. **36**, 1433 (2006).
[37] A. Rényi, in *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability* (1960), pp. 547–561.
[38] K. S. Gibbons, M. Hoffman, and W. K. Wootters, Physical Review A **062101** (2004).
[39] A. Casaccino, E. F. Galvao, and S. Severini, Physical Review A **78**, 022310 (2008).
[40] F. Kittneh, **143**, 337 (1997).
[41] P. M. Cohn, *Basic Algebra – Groups, Rings and Fields* (Springer, 2003).
[42] A. K. Kwasniewski, J. Math. Phys. **26**, 2234 (1985).
[43] P. Lounesto, *Clifford Algebras and Spinors* (Cambridge University Press, 2001).
[44] S. Wehner, Ph.D. thesis, University of Amsterdam (2008), arXiv:0806.3483.
[45] Note that the entropy of performing a measurement corresponding to an orthonormal basis in dimension d can never exceed $\log d$, where the maximum is attained when the distribution over the outcomes is uniform $1/d$.
[46] Orthogonal with respect to the Hilbert-Schmidt inner product.

In this appendix, we provide the technical details of our construction.

Appendix A: Constructing the unitary U

It is well known that for any orthonormal transformation $T \in \mathrm{O}(2n)$ there exists a corresponding unitary transformation $U(T)$ [43], where we refer to [44, Appendix C] for instructions on how to obtain explicit constructions. The transformation we wish to construct here, of the form $U(T)\Gamma_j U(T)^\dagger \to \Gamma_k$, is thereby particularly simple to obtain. It can be build up from successive rotations in the plane spanned by only two "vectors" Γ_j and Γ_k. More specifically, we first construct a unitary that corresponds to a rotation around an angle $\pi/2$ in the plane spanned by Γ_j and Γ_k, bringing Γ_j to Γ_k. This is simply a reflection around the plane orthogonal to the midvector between Γ_j and Γ_k, followed by a reflection around the plane orthogonal to Γ_k. Using the geometric properties of the Clifford algebra this corresponds to the unitary

$$R_{j\to k} = \Gamma_k(\Gamma_j + \Gamma_k)/\sqrt{2} \ . \tag{A1}$$

To obtain the desired unitary, we now compose a number of such rotations. Let $\hat{R}_{j,k} = R_{j\to k}$ if k is odd, and $\hat{R}_{j,k} = R_{k\to j}$ if k is even. Furthermore, let $F = \mathbb{I}$ if L is odd, and $F = \Gamma_{2n}\Gamma_{L-1}$ if L is even. Note that $\Gamma_{2n}\Gamma_{L-1}$ is the unitary that flips the sign of Γ_{L-1}, but leaves all Γ_j for $j \neq 2n$ and $j \neq L-1$ invariant. We may then write

$$U(T) = F\hat{R}_{0,1}\hat{R}_{0,2}\ldots\hat{R}_{0,L-1} \ . \tag{A2}$$

This transformation hence transforms $\Gamma_0 \to \Gamma_1 \to \ldots \to \Gamma_{L-1} \to \Gamma_0$, but leaves all other generators Γ_j for $j \geq L$ invariant. A similar unitary can be found for any transformation $T \in \mathrm{SO}(2n+1)$ [24], but is more difficult to construct explicitly.

Appendix B: Constructing maximally commuting classes of Clifford generators

In (17) and (18) we gave examples of constructing $L = 3$ and $L = 4$ MUBs in dimension $d = 4$, such that they are cyclically permuted under the action of a unitary U that permutes the Clifford generators in $d = 4$. Here, we show by a general construction that it is always possible to construct L such classes in dimension $d = 2^n$, whenever $L|n$ and L is prime. We also outline a construction for

$L = 2n+1$ classes, given a unitary U that cycles through *all* $2n+1$ Clifford generators, when $2n+1$ is prime.

Given the $2n$ generators of the Clifford algebra in dimension $d = 2^n$, we consider the set

$$\mathcal{S} = \{\mathbb{I}, \Gamma_j, i\Gamma_j\Gamma_k, \Gamma_j\Gamma_k\Gamma_l, ..., i\Gamma_0\Gamma_1..\Gamma_{2n-1} \equiv \Gamma_{2n}\}. \tag{B1}$$

To generate a set of $L \leq 2n+1$ MUBs, we seek to group the elements of $\mathcal{S}$ into L classes of commuting operators, ie. sets $\{\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{L-1} \mid \mathcal{C}_j \subset \mathcal{S}\backslash\{\mathbb{I}\}\}$ of size $|\mathcal{C}_j| = d-1$ such that

(**P1**) The elements of $\mathcal{C}_j$ commute for all $0 \leq j \leq L-1$,

(**P2**) The classs are all *mutually disjoint*, that is,

$$\mathcal{C}_j \cap \mathcal{C}_k = \emptyset \text{ for all } j \neq k, \tag{B2}$$

(**P3**) The unitary U that cyclically permutes the generators $\Gamma_0, \ldots, \Gamma_{L-1}$, also permutes the corresponding classes by permuting products of operators appropriately.

Our approach in obtaining such a set of classes is to first pick $d-1$ elements for the class $\mathcal{C}_0$ and then generate the rest of the classes by repeated application of U to the elements of $\mathcal{C}_0$. This automatically ensures property (**P3**). To ensure (**P1**) and (**P2**), the $d-1$ operators $\mathcal{C}_0 \equiv \{\mathcal{O}_1, \mathcal{O}_2, \ldots \mathcal{O}_{d-1}\}$ must satisfy the following:

(i) For any pair $\mathcal{O}_i, \mathcal{O}_j \in \mathcal{C}_0$, $[\mathcal{O}_i, \mathcal{O}_j] = 0$, and

(ii) The operators in $\mathcal{C}_0$ cycle through *mutually disjoint* sets of operators under the action of U.

To understand condition (ii) better, consider an operator $\mathcal{O}_i$ in $\mathcal{C}_0$. Then, by construction, $U^k(\mathcal{O}_i) \in \mathcal{C}_k$ for $0 \leq k \leq L-1$, assuming we construct a total of L classes. In addition, property (ii) implies $U^k(\mathcal{O}_i) \notin \mathcal{C}_j$, for any $j \neq k$. In other words, given any two operators $\mathcal{O}_i, \mathcal{O}_j \in \mathcal{C}_0$ that cycle through the sets

$$S_i = \{U^k(\mathcal{O}_i) | 0 \leq k \leq L-1\} \text{ and} \tag{B3}$$
$$S_j = \{U^k(\mathcal{O}_j) | 0 \leq k \leq L-1\}, \tag{B4}$$

respectively under the action of U, property(ii) demands that $S_i \cap S_j = \emptyset$, for all $i \neq j$ and $i, j = 1, 2, \ldots, d-1$.

Finally, we note that no class can contain two generators Γ_j and Γ_k, since they do not commute. When forming the classes we hence ensure that each one contains exactly one generator Γ_j, which we refer to as the *singleton* Γ-operator of the class, as opposed to the rest of the elements which will be *products* of Γ-operators. The fact that each class can contain at most one singleton operator limits us to constructing a maximum of $2n+1$ such classes.

1. Mathematical tools

Before proceeding to outline our construction, we establish some useful mathematical facts which will help motivate our algorithm for the construction of mutually disjoint classes. For the rest of the section, we will work with a set of p Γ-operators $\{\Gamma_0, \Gamma_2, \ldots, \Gamma_{p-1}\}$ that are cycled under the action of U, as follows,

$$U : \Gamma_0 \to \Gamma_1 \to \ldots \Gamma_{p-1} \to \Gamma_0, \tag{B5}$$

In other words, we are given a set of Γ-operators whose *cycle-length* is p.

2. Length-2 operators

First, we consider sets of products of two Γ-operators of the form $\Gamma_i\Gamma_j$, which we call *length-2* operators. It is convenient to characterize such pairs in terms of the *spacing* – (S) – between the operators that constitute them. The spacing function S, for given set of p operators, is simply defined as: $S(\Gamma_i\Gamma_j) = (j-i) \bmod p$. Then, the following holds:

Lemma B.1 (**Unique spacings imply non-intersecting cycles**). *The action of U on any length-2 operator $\Gamma_i\Gamma_j$ leaves its spacing function $S(.)$ invariant. Thus, length-2 operators that have unique spacings cycle through mutually disjoint sets of operators under the action of U.*

Proof. Recall, $U : \Gamma_i \to \Gamma_{(i+1) \bmod p}$. It clearly follows that

$$\begin{aligned} U : S(\Gamma_i\Gamma_j) &\to S\left(\Gamma_{(i+1) \bmod p}\Gamma_{(j+1) \bmod p}\right) \\ &= (j-i) \bmod p \\ &= S(\Gamma_i\Gamma_j). \end{aligned} \tag{B6}$$

□

3. Higher length operators

Similar to defining length-2 operators, we refer to any product of ℓ Γ-operators as a *length-ℓ* operator. For operators of length higher than 2, it becomes convenient to refer to them using their corresponding index sets. For example, the operator $\Gamma_{i_1}\Gamma_{i_2}\ldots\Gamma_{i_\ell}$ will be simply denoted by the index set $(i_1, i_2, \ldots i_\ell)$. In the following Lemma, we obtain a condition for any set of length-ℓ operators to cycle through mutually disjoint sets under the action of U.

Lemma B.2 (**Mutually disjoint cycles for length ℓ**). *Suppose the length-ℓ operators (for $3 \leq \ell \leq p-1$) that belong to the class $\mathcal{C}_0$ are such that they correspond to index sets $(i_1, i_2, \ldots, i_\ell)$ which all sum to the same value*

$$i_1 + i_2 + \ldots + i_\ell = c_\ell \, mod \, p, \; \forall \; (i_1, i_2, \ldots, i_\ell) \in \mathcal{C}_0 \tag{B7}$$

Then, no given index set of length ℓ can belong to more than one class, for prime values of p.

Proof. Given the operators $\{\Gamma_{i_1}\Gamma_{i_2}\ldots\Gamma_{i_\ell}\} \in \mathcal{C}_0$, such that the corresponding sets of indices $(i_1, i_2, \ldots, i_\ell)$ sum to

$$i_1 + i_2 + \ldots + i_\ell = c_\ell \bmod p,\ \forall (i_1, i_2, \ldots, i_\ell) \in \mathcal{C}_0. \quad \text{(B8)}$$

Under the action of U, these index sets changes to

$$\begin{aligned}(i_1, i_2, \ldots, i_\ell) \ &\rightarrow\ (i_1^{(1)}, i_2^{(1)}, \ldots, i_\ell^{(1)}) \\ &=\ (i_1 + 1, i_2 + 1, \ldots, i_\ell + 1) \bmod p\ .\end{aligned} \quad \text{(B9)}$$

For any index set $(i_1^{(1)}, i_2^{(1)}, \ldots, i_\ell^{(1)}) \in \mathcal{C}_1$ the sum of the indices corresponding to the new operators $\{\Gamma_{i_1^{(1)}}\Gamma_{i_2^{(1)}}\ldots\Gamma_{i_\ell^{(1)}}\} \in \mathcal{C}_1$ becomes

$$i_1^{(1)} + i_2^{(1)} + \ldots + i_\ell^{(1)} \ =\ (c_\ell + \ell) \bmod p, \quad \text{(B10)}$$

Proceeding similarly, the corresponding operators in the class $\mathcal{C}_k$ have index sets $(i_1^{(k)}, i_2^{(k)}, \ldots, i_\ell^{(k)})$ that sum to

$$i_1^{(k)} + i_2^{(k)} + \ldots + i_\ell^{(k)} \ =\ (c_\ell + k\ \ell) \bmod p, \quad \text{(B11)}$$

for all $(i_1^{(k)}, i_2^{(k)}, \ldots, i_\ell^{(k)}) \in \mathcal{C}_k$. Thus, starting with a constraint on the length-ℓ operators in $\mathcal{C}_0$, we have obtained a constraint on the corresponding operators in a generic class $\mathcal{C}_k$.

Now, suppose by contradiction an index set $(j_1, j_2, \ldots, j_\ell)$ whose indices $\{j_m\}_m$ take values from the set $\{0, 1, \ldots, p-1\}$, belongs to two different classes, $\mathcal{C}_k$ and $\mathcal{C}'_k$ (with $k \neq k'$). The constraint imposed by (B11) implies

$$\begin{aligned}(c_\ell + k\ \ell) \bmod p \ &=\ (c_\ell + k'\ \ell) \bmod p \\ \Rightarrow (k - k')\ell \bmod p \ &=\ 0.\end{aligned} \quad \text{(B12)}$$

Without loss of generality, let $k > k'$. Since we can form at most p classes, the difference $(k - k')$ can be at most $(p-1)$. Finally, note that since $\ell \leq p-1$, condition (B12) cannot be satisfied for prime values of p. □

Recall that our approach to constructing any p classes is to first construct the class $\mathcal{C}_0$, and then obtain the rest by successive application of U. Therefore, the fact that any index set of a certain length ℓ cannot belong to more than one class implies that each length-ℓ operator in $\mathcal{C}_0$ cycles through a unique set of length-ℓ operators under U. In other words, the length-ℓ operators cycle through mutually disjoint sets, as desired.

Lemma B.2 thus provides us with a sufficient condition for the set of length-ℓ operators in $\mathcal{C}_0$ to cycle through mutually disjoint sets under U, given a set of Γ-operators whose cycle-length is prime-valued. We only need to ensure that the length-ℓ operators in the first class that we construct, $\mathcal{C}_0$, correspond to index sets that *all* sum to the same value. This condition is of course subject to the constraint that the maximum allowed length for the operators in $\mathcal{C}_0$ (and by extension, in any class) is $p - 1$.

4. Constructing $2n + 1$ prime classes

As a warmup, we construct $L = 2n + 1$ classes in dimension $d = 2^n$, when $2n + 1$ is prime. This case is particulary easy, and illustrates how the results of the previous sections will be used in general.

Theorem B.3 ($2n + 1$ **prime classes**). *Let $\mathcal{G}^{(full)} = \{\Gamma_0, \ldots, \Gamma_{2n}\}$ denote the complete set of $2n + 1$ Γ-operators, and let U be the unitary that cycles through all of them, that is,*

$$U\ :\ \Gamma_0 \rightarrow \Gamma_1 \ldots \Gamma_{2n-1} \rightarrow \Gamma_{2n} \rightarrow \Gamma_0\ . \quad \text{(B13)}$$

*If $2n + 1$ is prime, then there exist $2n + 1$ classes $\mathcal{C}_0, \mathcal{C}_1, \ldots \mathcal{C}_{2n}$ satisfying properties **(P1)** through **(P3)**.*

Proof. We prove the existence of $2n + 1$ classes by construction. We first outline an algorithm to pick $d - 1$ operators that constitute the class $\mathcal{C}_0$. The remaining classes are easily obtained by the application of U to the elements of $\mathcal{C}_0$. Then, we make use of Lemmas B.1 and B.2 to prove that the classes obtained through our construction do satisfy the desired properties.

Algorithm

1. Pick one of the elements of $\mathcal{G}^{(\text{full})}$, Γ_0, as the singleton operator.

2. Pair up the remaining operators in $\mathcal{G}^{(\text{full})}$ to form $(n-1)$ length-2 operators which commute with Γ_0, as follows,

$$\begin{aligned}\mathcal{L}_2 \ =\ \{&\Gamma_1\Gamma_{2n},\ \Gamma_2\Gamma_{2n-1},\ \ldots, \\ &\ldots, \Gamma_{n-2}\Gamma_{n+3},\ \Gamma_{n-1}\Gamma_{n+2}\},\end{aligned} \quad \text{(B14)}$$

   where $\mathcal{L}_2$ denotes the set of length-2 operators in $\mathcal{C}_1$. Since we have left out the pair $\Gamma_n\Gamma_{n+1}$ in the middle, we get, $|\mathcal{L}_2| = n - 1$.

3. Form higher length operators that commute with $\mathcal{L}_2 \cup \{\Gamma_0\}$, by combining Γ_0 with appropriate combinations of the length-2 operators. Any operator of even length $\ell = 2j$ is created by combining i pairs in $\mathcal{L}_2$. And any operator of odd length $\ell = 2j+1$ is created by appending Γ_0 to a length-$2j$ operator.

   Denoting the sets of length-3 operators as $\mathcal{L}_3$, length-4 operators as $\mathcal{L}_4$, and in general, the set of length-i operators as $\mathcal{L}_i$, we have,

$$\begin{aligned}|\mathcal{L}_3| \ &=\ |\mathcal{L}_2| = n - 1, \\ |\mathcal{L}_4| \ &=\ \binom{n-1}{2},\ |\mathcal{L}_5| = |\mathcal{L}_4|, \\ |\mathcal{L}_6| \ &=\ \binom{n-1}{3},\ |\mathcal{L}_7| = |\mathcal{L}_6|, \\ &\vdots \quad\ \vdots \\ |\mathcal{L}_{2n-2}| \ &=\ \binom{n-1}{n-1} = 1,\ |\mathcal{L}_{2n-1}| = |\mathcal{L}_{2n-2}|.\end{aligned}$$

Putting together the operators from 1, 2, and 3 we get the desired cardinality for the class $\mathcal{C}_0$ -

$$\begin{aligned}|\mathcal{C}_0| &= 1+(n-1)+\sum_{i=3}^{2n}|\mathcal{L}_i| \\ &= 1+2(n-1)+2\left(\begin{array}{c} n-1 \\ 2 \end{array}\right)+2\left(\begin{array}{c} n-1 \\ 3 \end{array}\right) \\ &\quad +...+2\left(\begin{array}{c} n-1 \\ n-1 \end{array}\right) \\ &= 2\sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right)-1 = 2(2^{n-1})-1 \\ &= 2^n-1 = d-1 \end{aligned} \tag{B15}$$

The rest of the classes are generated by successive applications of the unitary U to the elements of $\mathcal{C}_0$, so that $U:\mathcal{C}_i \to \mathcal{C}_{(i+1) \mod 2n+1}$.

It is easy to see that the elements of each class satisfy property (**P1**) above – the different length operators have been picked in such a way as to ensure that they all commute with each other. Similarly, by construction, they satisfy property **(P3)**. It only remains to prove property (**P2**), that the classes are all mutually disjoint.

The elements of $\mathcal{L}_2$ correspond to the following set of spacings

$$S(\mathcal{L}_2) \equiv \{2n-1, 2n-3, \ldots, 5, 3\} \tag{B16}$$

which are all distinct. So by Lemma B.1, the elements of $\mathcal{L}_2$ cycle through mutually disjoint sets of length-2 operators.

For higher length operators, we first show that our construction meets the conditions of Lemma B.2. For the class $\mathcal{C}_0$, the elements of $\mathcal{L}_2$ correspond to index sets that satisfy

$$\mathcal{L}_2(\mathcal{C}_0) = \{(i_1,i_2)|\, i_1+i_2 = 0 \bmod (2n+1)\}. \tag{B17}$$

The length-2 operators of a generic class $\mathcal{C}_k$ similarly satisfy

$$\mathcal{L}_2(\mathcal{C}_k) = \{(i_1,i_2)|\, i_1+i_2 = 2k \bmod (2n+1)\}. \tag{B18}$$

Since higher length operators are essentially combinations of length-2 operators and the singleton operator, conditions similar to (B18) hold for higher length index sets as well. Since operators of even length $2j$ contain j pairs from $\mathcal{L}_2$, the corresponding index sets in $\mathcal{C}_0$ satisfy

$$\begin{aligned} i_1+i_2+\ldots+i_{2j} &= 0 \bmod (2n+1), \\ &\forall\ (i_1,i_2,\ldots,i_{2j}) \in \mathcal{C}_0. \end{aligned} \tag{B19}$$

Similarly, since the odd length operators have Γ_0 appended to the even length operators, the index sets of length $2j+1$ in $\mathcal{C}_0$ satisfy,

$$\begin{aligned} i_1+i_2+\ldots+i_{2j+1} &= 0 \bmod (2n+1), \\ &\forall\ (i_1,i_2,\ldots,i_{2j+1}) \in \mathcal{C}_0. \end{aligned} \tag{B20}$$

To sum up, for any $3 \le \ell \le 2n$, our construction ensures that index sets of length ℓ belonging to $\mathcal{C}_0$ sum to the same value. The conditions of Lemma B.2 are therefore satisfied, with the quantity c_ℓ in (B7) taking the value $c_\ell = 0$, for all $\ell = 3,\ldots,2n$. Now, we can simply evoke Lemma B.2 to prove that, when $2n+1$ is prime, the higher length operators in $\mathcal{C}_0$ cycle through mutually disjoint sets of operators. □

5. Constructing $L|n$ classes for prime values of L

Next, we show that is possible to obtain an arrangement of operators into L classes in dimension 2^n, when L is prime and $L|n$, such that the unitary U that cyclically permutes L Γ-operators also permutes the coresponding classes.

Theorem B.4 ($L|n$ **classes for prime** L)**.** *Suppose U is a unitary that cycles through sets of L Γ-operators from the set $\mathcal{G}^{(full)} \setminus \{\Gamma_{2n}\}$ in dimension 2^n, where L is prime and $L|n$. Then there exist L classes $\mathcal{C}_0, \mathcal{C}_1, \ldots \mathcal{C}_{L-1}$ that satisfy properties **(P1)** through **(P3)**.*

Proof: Note that since $L|n$ we have $n = rL$ for some positive integer r. The set of $2n$ Clifford generators $\Gamma_0, \Gamma_1, \ldots, \Gamma_{2n-1}$ can then be partitioned into $2r$ sets as follows:

$$\begin{aligned} \mathcal{G}^{(0)} &= \{\Gamma_0, \Gamma_1, \ldots, \Gamma_{L-1}\}, \\ \mathcal{G}^{(1)} &= \{\Gamma_L, \Gamma_{L+1}, \ldots, \Gamma_{2L-1}\}, \\ &\vdots \quad \vdots \\ \mathcal{G}^{(2r-1)} &= \{\Gamma_{(2r-1)L}, \Gamma_{(2r-1)L+1}, \ldots, \Gamma_{2n-1}\} \end{aligned} \tag{B21}$$

Without loss of generality, we can assume the unitary U is constructed such that it cyclically permutes the L operators within each set, as follows.

$$\begin{aligned} U\ :\ & \Gamma_0 \to \Gamma_1 \to \ldots \to \Gamma_{L-1} \to \Gamma_0, \\ & \Gamma_L \to \ldots \to \Gamma_{2L-1} \to \Gamma_L, \\ & \vdots \\ & \Gamma_{(2r-1)L} \to \ldots \to \Gamma_{2n-1} \to \Gamma_{(2r-1)L}. \end{aligned}$$

Once again, we begin with an algorithm for picking $d-1$ elements for the class $\mathcal{C}_0$. The algorithm closely follows the one outlined in the previous section, barring some minor modifications.

Algorithm

1. The "middle" element from $\mathcal{G}^{(1)}$, $\Gamma_{(L-1)/2}$, is picked as the singleton element of $\mathcal{C}_0$.

2. The $(n-1)$ length-2 operators which commute with $\Gamma_{(L-1)/2}$ are picked as follows –

(a) $\frac{L-3}{2}$ pairs are picked from $\mathcal{G}^{(0)} \setminus \{\Gamma_{(L-1)/2}\}$

$$\mathcal{L}_2^{(0)} = \{\,\Gamma_1\Gamma_{L-1},\, \Gamma_2\Gamma_{L-2}, \ldots, \Gamma_{(L-3)/2}\Gamma_{(L+3)/2}\,\},$$

leaving Γ_0 and $\Gamma_{(L+1)/2}$ unused.

(b) $\frac{L-1}{2}$ pairs are picked from each of the sets $\mathcal{G}^{(1)}$ through $\mathcal{G}^{(2r-1)}$,

$$\begin{aligned}
\mathcal{L}_2^{(1)} &= \{\,\Gamma_{L+1}\Gamma_{2L-1},\, \Gamma_{L+2}\Gamma_{2L-2},\, \ldots, \\
&\qquad \ldots,\, \Gamma_{L+(L-1)/2}\Gamma_{L+(L+1)/2}\,\}, \\
&\vdots \quad \vdots \\
\mathcal{L}_2^{(2r-1)} &= \{\,\Gamma_{(2r-1)L+1}\Gamma_{2n-1},\, \Gamma_{(2r-1)L+2}\Gamma_{2n-2},\, \ldots, \\
&\qquad \Gamma_{(2r-1)L+(L-1)/2}\Gamma_{(2r-1)L+(L+1)/2}\,\},
\end{aligned}$$

leaving the first operator in each set unused.

(c) Finally, the unused Γ-operators from different sets are put together as specified below, to get the remaining r length-2 operators:

$$\mathcal{L}_2^{(2r)} = \{\,\Gamma_0\Gamma_L,\, \Gamma_{2L}\Gamma_{3L}, \ldots, \Gamma_{(2r-2)L}\Gamma_{(2r-1)L}\,\}.$$

The set of length-2 operators is then given by

$$\mathcal{L}_2 = \mathcal{L}_2^{(0)} \cup \mathcal{L}_2^{(1)} \ldots \cup \mathcal{L}_2^{(2r-1)} \cup \mathcal{L}_2^{(2r)}$$

which gives $|\mathcal{L}_2| = \frac{L-3}{2} + (2r-1)\left(\frac{L-1}{2}\right) + r = rL - \frac{2r-2}{2} + r = n-1$.

3. Pick higher length operators from $\mathcal{S}$ that commute with $\Gamma_{(L-1)/2}$ and $\mathcal{L}_2$, by combining $\Gamma_{(L-1)/2}$ with appropriate combinations of the length-2 operators. As before, any even-length operator of length $\ell = 2i$ is obtained by combining i length-2 operators from $\mathcal{L}_2$. Any operator of odd-length $\ell = 2i+1$, is created by appending $\Gamma_{(L-1)/2}$ to a length-$2i$ operator.

Putting together all the operators created in Steps[1]-[3], we get the desired cardinality for the class (see (B15)), that is, $|\mathcal{C}_0| = 2^n - 1$.

Proof of properties (P1) through (P3): The different length operators have again been picked in such a way as to ensure that they all commute with each other. Since the remaining $L-1$ classes are generated by successive applications of the unitary U to the elements of $\mathcal{C}_0$, we have $U : \mathcal{C}_i \to \mathcal{C}_{(i+1) \bmod L}$. Thus **(P1)** and **(P3)** is satisfied. It remains to prove that the classes constructed here also satisfy property (**P2**).

As in the earlier case of $2n+1$ classes, the operators in each of the sets $\{\mathcal{L}_2^{(0)}, \mathcal{L}_2^{(1)}, \ldots, \mathcal{L}_2^{(2r-1)}\}$ correspond to unique values of the spacing function:

$$S(\mathcal{L}_2^{(i)}) \equiv \{L-2, L-4, \ldots, 1\}, \forall i \in [0, 2r-1],$$

which guarantees, by Lemma B.1 that these operators cycle through mutually disjoint sets under U. Since the operators in $\mathcal{L}_2^{(2r)}$ are formed by combining Γ-operators from different sets $\mathcal{G}^{(i)}$, each of them cycles through a different set of operators under U. Thus we see that all the length-2 operators in $\mathcal{C}_0$ cycle through mutually disjoint sets.

Before we proceed to discuss the higher length operators, we make one further observation about the length-2 operators. The operators in $\mathcal{L}_2$ correspond to index sets which satisfy

$$\mathcal{L}_2(\mathcal{C}_1) = \{\Gamma_{i_1}\Gamma_{i_2} |\, i_1 + i_2 = 0 \bmod L\}.$$

In particular, the length-2 operators in the set $\mathcal{L}^{(2r)}$ have been picked carefully so as to ensure that the above constraint is satisfied. In fact, this was the rationale behind leaving out the first operator in each of the sets $\mathcal{G}^{(i)}$ while choosing the corresponding length-2 elements in $\mathcal{L}_2^{(i)}$.

The higher length operators in $\mathcal{C}_0$ can be of two types:

(a) Those that are comprised of Γ-operators from a single set $\mathcal{G}^{(i)}$ alone, and

(b) Operators that comprise Γ-operators from more than one set.

Since a type-(a) operator cannot cycle into a type-(b) operator under the action of U, these two cases can be examined separately.

Type-(a): The maximum length that an operator of type-(a) can have, as per our construction, is $L-1$. We have ensured this by leaving at least one operator of each of the sets $\mathcal{G}^{(i)}$ unused in constructing the length-2 operators. Furthermore, the constraint in (B22) implies that the index sets corresponding to such higher length operators in $\mathcal{C}_0$, sum to the same value modulo L. More precisely, any even-length index set of length $\ell = 2j$, where the indices are all drawn from a given set $\mathcal{G}^{(i)}$, satisfies

$$\begin{aligned}
i_1 + i_2 + \ldots + i_l &= 0 \bmod L, \\
&\forall\ (i_1, i_2, \ldots, i_l) \in \mathcal{C}_0. \qquad \text{(B22)}
\end{aligned}$$

And any index set of odd length $\ell = 2j+1$ satisfies

$$\begin{aligned}
i_1 + i_2 + \ldots + i_l &= \left(\frac{L-1}{2}\right) \bmod L, \\
&\forall\ (i_1, i_2, \ldots, i_l) \in \mathcal{C}_0. \qquad \text{(B23)}
\end{aligned}$$

Then, invoking Lemma B.2 with $c_\ell = 0$ for even values of ℓ and $c_\ell = (L-1)/2$ for odd values of ℓ, we see that no operator of type-(a) can belong to more than one class, for prime values of L.

Type-(b): An operator of type-(b) is a product of operators from smaller sets $\mathcal{K}_j \subseteq \mathcal{G}^{(j)}$. Consider a length-$\ell$ operator, $\mathcal{O}$ which comprises ℓ_0 Γ-operators from $\mathcal{G}^{(0)}$, ℓ_1 operators from $\mathcal{G}^{(1)}$, and in general, ℓ_i from the set $\mathcal{G}^{(i)}$.

$$\mathcal{O} = \underbrace{\Gamma_{i_1} \ldots \Gamma_{i_{\ell_0}}}_{\mathcal{K}_0 \subseteq \mathcal{G}^{(0)}} \underbrace{\Gamma_{j_1} \ldots \Gamma_{j_{\ell_1}}}_{\mathcal{K}_1 \subseteq \mathcal{G}^{(1)}} \ldots \underbrace{\Gamma_{k_1} \ldots \Gamma_{k_{\ell_{2r-1}}}}_{\mathcal{K}_{2r-1} \subseteq \mathcal{G}^{(2r-1)}}$$

Note that by our construction, the operator $\mathcal{O}$ exists in more than one class if and only if, for all $\mathcal{K}_j$ the product of all operators in $\mathcal{K}_j$ also belongs to more than one class. In what follows, we argue that our construction ensures that this is not possible. In particular, given a set of length-ℓ operators in $\mathcal{C}_0$ which can be broken down into smaller sets as described above, we will argue that there exists at least one set $\mathcal{K}_j$ in every such length-ℓ operator $\mathcal{O}$, such that the products of operators in $\mathcal{K}_j$ corresponding to different length-ℓ operators cycle through mutually disjoint sets, as defined earlier.

Note the following two facts about the subsets $\mathcal{K}_j$. First, our construction ensures that any subset $\mathcal{K}_j \subseteq \mathcal{G}^{(j)}$ of a given size ℓ_j, satisfies either (B22) or (B23) depending on ℓ_j being even or odd. Second, note that the maximum size of these subsets is $\ell_j \leq L$. However, in order to invoke Lemma B.2, we still require ℓ_j to be strictly less than L. Our goal is hence to show that every length-ℓ operator must have at least one subset $\mathcal{K}_j$ of size $\ell_j < L$.

Suppose there exists a length-ℓ operator such that every subset is of size L. Then, the operator itself has to be of length

$$\ell = \ell_0 + \ell_1 + \ldots + \ell_{2r-1} = 2rL = 2n \tag{B24}$$

However the maximum value of ℓ in our construction is $2n-1$, implying that atleast one of the $2r$ subsets must be of a size strictly smaller than L. And, for such a subset of size less than L, constraints (B22) and (B23) ensure that the same subset cannot be found in more than one class, provided L is prime. □

Appendix C: A simple lower bound on min-entropy

The min-entropy of the distribution that an orthonormal basis $\mathcal{B}_j = \{|b^{(j)}\rangle\}_b$ induces on a state $\rho \in \mathcal{H}$ is given by

$$\mathcal{H}_\infty(\mathcal{B}_j|\rho) = -\log \max_b \mathrm{Tr}[|b^{(j)}\rangle\langle b^{(j)}|\rho] \tag{C1}$$

We are looking to evaluate a lower bound on the average min-entropy of any L mutually unbiased bases (not necessarily coming from our construction) in a d-dimensional Hilbert space. The average min-entropy is given by -

$$\begin{aligned} \frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j|\rho) &= -\frac{1}{L}\sum_j \log \max_{b^{(j)}\in\{0,\ldots,d-1\}} \langle b^{(j)}|\rho|b^{(j)}\rangle \\ &\geq -\log \frac{1}{L}\sum_{j=0}^{L-1} \max_{b^{(j)}} \langle b^{(j)}|\rho|b^{(j)}\rangle \end{aligned} \tag{C2}$$

using Jensen's inequality. The problem of finding an optimal uncertainty relation for the min-entropy, thus reduces to the problem of maximizing over all $\rho \in \mathcal{H}$, the quantity $\sum_{j=0}^{L-1} \max_{b^{(j)}\in\{0,\ldots,d-1\}} \langle b^{(j)}| \rho |b^{(j)}\rangle$. It is easy to see that this maximum is always attained at a pure state, so we can restrict the problem to an optimization over pure states. We can simplify the problem of finding the lower bound of (C2) by recasting it as follows.

Consider states of the form $P_{\vec{b}} = \frac{1}{L}\sum_{j=0}^{L-1} |b^{(j)}\rangle\langle b^{(j)}|$ where $\vec{b} = (b^{(0)}, b^{(1)}, ..., b^{(L-1)})$ denotes a string of basis elements, that is, $b^{(j)} \in \{0, 1, ..., d-1\}$. Suppose we can show for all possible strings $\vec{b}$,

$$\max_{|\psi\rangle} \mathrm{Tr}(P_{\vec{b}}|\psi\rangle\langle\psi|) \leq \zeta \ . \tag{C3}$$

Then, since $\frac{1}{L}\sum_j |\langle b^{(j)}|\psi\rangle|^2 = \mathrm{Tr}[P_{\vec{b}}|\psi\rangle\langle\psi|]$, the bound is simply

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle\langle\psi|) \geq -\log\zeta \ . \tag{C4}$$

We have thus reduced the problem to one of finding the maximum eigenvalue of operators of the form $P_{\vec{b}}$, over all possible strings $\vec{b}$.

1. A new bound for smaller sets of $L < d$ MUBs

We now prove Lemma III.2, restated here for convenience.

Lemma C.1. *Let $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ be a set of mutually unbiased bases in dimension $d = 2^n$. Then*

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right] \ . \tag{C5}$$

Proof. Note that by (C4), it is sufficient to determine ζ in (C3). To solve this eigenvalue problem we recall a result of Schaffner [30] proved using the methods of Kittaneh [40], that for a set of L orthogonal projectors $A_0, A_1, \ldots, A_{L-1}$, the following bound holds:

$$\| \sum_{j=0}^{L-1} A_j \| \leq 1 + (L-1) \max_{0\leq j<k\leq L-1} \| A_j A_k \| \tag{C6}$$

where $\| (.) \|$ denotes the operator norm, which here is simply the maximum eigenvalue for Hermitian operators. Applying this result to sums of basis vectors $|b^{(j)}\rangle$, we have,

$$\begin{aligned} \| \sum_{j=0}^{L-1} |b^{(j)}\rangle\langle b^{(j)}| \| \ &\leq \ 1 + \\ &(L-1) \max_{0\leq j<k\leq L-1} \| (|b^{(j)}\rangle\langle b^{(j)}|)(|b^{(k)}\rangle\langle b^{(k)}|) \| \end{aligned} \tag{C7}$$

which implies

$$\begin{aligned} \| P_{\vec{b}} \| \ &\leq \ \frac{1}{L} + \\ &\left(\frac{L-1}{L}\right) \max_{0\leq j<k\leq L-1} \| \ |b^{(j)}\rangle(\langle b^{(j)}||b^{(k)}\rangle)\langle b^{(k)}| \ \| \end{aligned} \tag{C8}$$

(C9)

Recall, that for all $b^{(j)}, b^{(k)} \in \{0, \ldots, d-1\}$

$$\langle b^{(j)}|b^{(k)}\rangle = e^{i\phi}\frac{1}{\sqrt{d}}, \text{ for any } j \neq k, \tag{C10}$$

where ϕ denotes some phase factor. Further, since the vectors $|b^{(j)}\rangle$ are normalized, the Cauchy-Schwarz inequality gives

$$\| \, |b^{(j)}\rangle\langle b^{(k)}| \, \| \leq 1, \text{ for any } b^{(j)}, b^{(k)} \in \{0, \ldots, d-1\}. \tag{C11}$$

Combining these with (C8) gives the following bound on the maximum eigenvalue of the operator $P_{\vec{b}}$:

$$\zeta = \frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right) . \tag{C12}$$

By (C4), this immediately proves our claim. □

2. A stronger bound for the complete set of $d+1$ MUBs

Here, we present an alternate approach to bound the maximum eigenvalue of $P_{\vec{b}}$, using a Bloch vector like representation of the MUB basis states. The bound that we obtain here, stated in Lemma III.3, is stronger than the last one when $L > d$. In particular, when we consider the complete set ($L = d+1$) of MUBs in any dimension d, this approach yields the best known bound.

Lemma C.2. *Let $\mathcal{B}_0, \ldots, \mathcal{B}_{L-1}$ be a set of mutually unbiased bases in dimension $d = 2^n$. Then*

$$\frac{1}{L}\sum_{j=0}^{L-1} \mathcal{H}_\infty(\mathcal{B}_j||\psi\rangle) \geq -\log\left[\frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\right] . \tag{C13}$$

Proof. First, we switch to working in a basis of Hermitian operators, so that every state in $\mathcal{H}$ has a parametrization in terms of vectors in a real vector space. Any state $\rho \in \mathcal{H}$ can be written as:

$$\rho = \frac{1}{d}\mathbb{I} + \frac{1}{2}\sum_{i=1}^{d^2-1} \alpha^{(i)}\hat{A}_i \tag{C14}$$

where $\{\hat{A}_i\}$ are Hermitian, trace-less operators that are orthogonal with respect to the Hilbert-Schmidt norm: $\mathrm{Tr}[\hat{A}_i^\dagger \hat{A}_j] = 2\,\delta_{ij}$, and the scalars $\{\alpha^{(i)}\}_i \in \mathbb{R}$. Thus we can parameterize any state in our d-dimensional Hilbert space with a vector $\vec{\alpha} = (\alpha^{(1)}, ..., \alpha^{(d^2-1)}) \in \mathbb{R}^{d^2-1}$. When ρ is a pure state ($\mathrm{Tr}[\rho^2] = 1$), the vector $\vec{\alpha}$ corresponding to this pure state satisfies the following normalization condition

$$\begin{aligned} \mathrm{Tr}\left[\left(\frac{1}{d}\mathbb{I} + \frac{1}{2}\sum_{i=1}^{d^2-1}\alpha^{(i)}\hat{A}_i\right)^2\right] &= 1 \\ \Rightarrow \frac{1}{d} + \frac{1}{2}\sum_{i=1}^{d^2-1}|\alpha^{(i)}|^2 &= 1 \\ \Rightarrow |\vec{\alpha}| = \sqrt{\sum_{i=1}^{d^2-1}|\alpha^{(i)}|^2} &= \sqrt{\frac{2(d-1)}{d}} \end{aligned} \tag{C15}$$

Furthermore, in this representation, the vectors $\{\vec{\alpha}_{(b,j)}\}$ corresponding to the MUB states $\{|b^{(j)}\rangle\}$ satisfy the following special properties:-

- (M1) *Normalization* - $\mathrm{Tr}[|b^{(j)}\rangle\langle b^{(j)}||b^{(j)}\rangle\langle b^{(j)}|] = 1$ implies that $|\vec{\alpha}_{(b,j)}| = \sqrt{\frac{2(d-1)}{d}}$, $\forall\ b = \{0, ..., d-1\}$, $j = \{0, ..., L-1\}$. (By an argument similar to the one that leads to (C15).)
- (M2) *Constant inner-product* - $|\langle b^{(j)}|\hat{b}^{(k)}\rangle|^2 = \frac{1}{d}$ implies that $\vec{\alpha}_{(b,j)}.\vec{\alpha}_{(\hat{b},k)} = 0$, $\forall\ j \neq k$, $\forall\ b, \hat{b} \in \{0, ..., d-1]$. This is easily seen, as follows:

$$\begin{aligned} \mathrm{Tr}[|b^{(j)}\rangle\langle b^{(j)}||b^{(k)}\rangle\langle b^{(k)}|] &= \frac{1}{d} + \frac{1}{2}\sum_i \alpha^{(i)}_{(b,j)}\alpha^{(i)}_{(\hat{b},k)} = \frac{1}{d} \\ \Rightarrow \vec{\alpha}_{(b,j)}.\vec{\alpha}_{(\hat{b},k)} &= 0 \end{aligned} \tag{C16}$$

Now, using this representation of MUB states and density operators, we can rewrite the maximization problem of (C3) as:

$$\begin{aligned} &\max_{|\psi\rangle} \mathrm{Tr}[P_{\vec{b}}|\psi\rangle\langle\psi|] = \max_{|\psi\rangle} \mathrm{Tr}\left[\frac{1}{L}\sum_j |b^{(j)}\rangle\langle b^{(j)}||\psi\rangle\langle\psi|\right] \\ &\leq \max_{\vec{\alpha}} \frac{1}{L}\sum_j \mathrm{Tr}\left[\left(\frac{\mathbb{I}}{d} + \frac{\sum_j \alpha^j_{(b^{(j)},j)}\hat{A}_j}{2}\right)\left(\frac{\mathbb{I}}{d} + \frac{\sum_i \alpha^{(i)}\hat{A}_i}{2}\right)\right] \\ &= \max_{\vec{\alpha}} \frac{1}{L}\sum_j \left(\frac{1}{d} + \frac{1}{2}\vec{\alpha}_{(b^{(j)},j)}.\vec{\alpha}\right) \\ &= \frac{1}{d} + \max_{\vec{\alpha}} \frac{1}{2L}\sum_j \vec{\alpha}_{(b^{(j)},j)}.\vec{\alpha} \end{aligned} \tag{C17}$$

Now we only need to find the real (d^2-1)-dimensional vector $\vec{\alpha}$, that maximizes the sum $\sum_j \vec{\alpha}_{(b^{(j)},j)}.\vec{\alpha}$. If we now define an "average" vector corresponding to each string $\vec{b}$, as follows

$$\frac{1}{L}\sum_j \vec{\alpha}_{(b^{(j)},j)} = \vec{\alpha}_{(\mathrm{avg})} \tag{C18}$$

then, it becomes obvious that the maximum is attained when $\vec{\alpha}$ is parallel to $\vec{\alpha}^{(\mathrm{avg})}$. Since it is a vector corresponding to a pure state, its norm is given by (C15), so

that

$$\vec{\alpha}_{(\max)} = \sqrt{\frac{2(d-1)}{d}} \frac{\vec{\alpha}_{(\text{avg})}}{|\vec{\alpha}_{(\text{avg})}|} \tag{C19}$$

Note that this maximizing vector has a constant overlap with all vectors $\vec{\alpha}^{(b^{(j)},j)}$, for a given string $\vec{b}$. In other words, for each string $\vec{b}$, the maximum is attained by the vector that makes equal angles with all the vectors that constitute the "average" vector ($\vec{\alpha}_{(\text{avg})}$) corresponding to that string. Note however that this vector may not always correspond to a state.

Now that we know the maximizing vector, we can go ahead and compute the value of ζ in (C3).

$$\begin{aligned}
\max_{|\psi\rangle} \text{Tr}[P_{\vec{b}}|\psi\rangle\langle\psi|] &\leq \frac{1}{d} + \max_{\vec{\alpha}} \frac{1}{2L} \sum_j \vec{\alpha}_{(b^{(j)},j)}.\vec{\alpha} \\
&= \frac{1}{d} + \frac{1}{2} \max_{\vec{\alpha}} \vec{\alpha}_{(\text{avg})}.\vec{\alpha} \\
&= \frac{1}{d} + \frac{1}{2} \frac{\vec{\alpha}_{(\text{avg})}.\vec{\alpha}_{(\text{avg})}}{|\vec{\alpha}_{(\text{avg})}|} \sqrt{\frac{2(d-1)}{d}} \\
&= \frac{1}{d} + \frac{1}{2} |\vec{\alpha}_{(\text{avg})}| \sqrt{\frac{2(d-1)}{d}} \\
&= \frac{1}{d} + \frac{1}{2\sqrt{L}} \frac{2(d-1)}{d} \\
&= \frac{1}{d} \left(1 + \frac{d-1}{\sqrt{L}}\right)
\end{aligned} \tag{C20}$$

where we have used the fact that the vector $\vec{\alpha}_{(\text{avg})}$ have a constant norm which can be computed as follows:

$$\begin{aligned}
\vec{\alpha}_{(\text{avg})}.\vec{\alpha}_{(\text{avg})} &= \frac{1}{L^2} \sum_{j,k} \vec{\alpha}^{(b^{(k)},k)}.\vec{\alpha}^{(b^{(j)},j)} \\
&= \frac{1}{L^2} \sum_j \vec{\alpha}_{(b^{(j)},j)}.\vec{\alpha}_{(b^{(j)},j)} \\
&= \frac{1}{L^2}(L) \left[\frac{2(d-1)}{d}\right] \\
\Rightarrow |\vec{\alpha}_{(\text{avg})}| &= \frac{1}{\sqrt{L}} \sqrt{\frac{2(d-1)}{d}},
\end{aligned} \tag{C21}$$

thus proving our claim. The second step follows from the fact that vectors corresponding to different MUB states have zero inner product (see property $(M2)$ above). □

Note that the fact that the bases are mutually unbiased was crucial in giving rise to properties $(M1)$ and $(M2)$ which in turn enabled us to identify the maximizing vector $\alpha_{\max}$. Indeed the maximizing vector corresponding to a given string $\vec{b}$ might not always correspond to a valid state, in which case the bound we derive cannot be achieved. However, there exist strings of basis elements $\vec{b}$, for which we can explicitly construct a state that has equal trace overlap with the states that constitute the corresponding operator $P_{\vec{b}}$. These are in fact states of the form

$$P_{\vec{b}} = \frac{1}{L} \sum_j |b^{(j)}\rangle\langle b^{(j)}|, \text{ where } \vec{b} = \{c, ..., c\}, \tag{C22}$$

for any $c \in \{0, \ldots, d-1\}$. Clearly, for the symmetric MUBs that we construct, an eigenstate of the unitary U that cycles between the different MUBs has the same trace overlap with each of the states $\{|b^{(j)}\rangle, j = 0, \ldots, L-1\}$, for a fixed value of b. To see this, suppose $|\phi\rangle$ is an eigenvector of U with eigenvalue λ, then for all $0 \leq j \leq L-1$ and a given value of b,

$$\begin{aligned}
\text{Tr}[|b^{(j)}\rangle\langle b^{(j)}||\phi\rangle\langle\phi|] &= |\langle b^{(j)}|\phi\rangle|^2 = |\langle b^{(1)}|(U^\dagger)^{j-1}|\phi\rangle|^2 \\
&= (|\lambda|^2)|\langle b^{(1)}|\phi\rangle|^2 \\
&= |\langle b^{(1)}|\phi\rangle|^2
\end{aligned} \tag{C23}$$

This is indeed the case for $L = 4$ MUBs in $d = 4$, where the lower bound we derive is achieved by eigenstates of U.