Abstract

I introduce a new notion, that extends the mutually unbiased bases (MUB) conditions to more than two bases. These, I call the nUB conditions, and the corresponding bases n-fold unbiased. They naturally appear while optimizing generic n-to-one quantum random access code (QRAC) strategies. While their existence in general dimensions is an open question, they nevertheless give close-to-tight upper bounds on QRAC success probabilities, and raise fundamental questions about the geometry of quantum states.

1 Introduction

Mutually unbiased bases (MUBs) are an important notion in quantum information theory, first studied in the context of optimal state-determination [1, 2]. Later, they found applications in entropic uncertainty relations [3], and surveys [4, 5]), information locking [6, 7] and the so-called Mean King’s problem [8, 9]. Intuitively speaking, if some classical information is encoded in a basis, then measuring in a basis unbiased to it reveals nothing about the encoded information whatsoever (see Section 2 for a formal definition). There is a great number of papers investigating the existence and constructions of these bases (see [10] for a survey, [11] for a classification in dimensions 2-5 and [12, 13, 14, 15, 16, 17] for the question of the number of MUBs in dimension 6). It is known that in any dimension, there are at least 3, and at most \( d + 1 \) MUBs, the upper bound being saturated in prime power dimensions. Composite dimensions on the other hand still remain unsolved.

While the bases are called mutually unbiased, the MUB conditions on \( n \) bases effectively impose only pairwise mutual unbiasedness. In this paper, I introduce a new notion, which is a global constraint on \( n \) bases, that I call \( n \)-fold unbiased bases (nUBs). These conditions naturally arise, while extending some methods of [18]. There, the authors prove that MUBs provide optimal measurements in the so-called quantum random access code (QRAC) protocol...
in the two-input case. $n$-fold unbiased bases then generalize this optimization task to $n$ inputs.

The above mentioned QRACs are a basic information theoretical protocol, used in many contexts within quantum information theory (for a comprehensive generic description, see [19]). Loosely speaking, the task is to compress $n$ dits into one (quantum) dit, and to be able to recover one randomly chosen dit with high probability (see Section 2 for a formal treatment). First, it appeared in [20], and was called conjugate coding. Later, it was studied in the context of quantum finite automata [21, 22, 23], quantum communication complexity [24, 25, 26, 27], network coding [28, 29], and locally decodable codes [30, 31, 32, 33]. Recently, it is used also for “quantumness witness”, that is, experimentally distinguishing different product structures of fixed dimensional systems [34]. Its versatile use is the consequence of its simplicity, and the fact that it provides quantum advantage over classical strategies.

The paper is organized as follows: in Section 2, I formally describe $n^d \rightarrow 1$ QRACs, and cite the result stating that MUBs are optimal in a $2^d \rightarrow 1$ QRAC scenario. In Section 3, I give a formal definition of $n$-fold unbiased bases, and state my main theorem about their optimality in $n^d \rightarrow 1$ QRACs, whenever $d \geq n$. Then, in Section 4, I give a rigorous proof of the main theorem. In Section 5, I address the problem of existence of $n$-fold unbiased bases with some rigorous results in low dimensions, but leaving the general question open. Section 6 focuses on applications, mainly considering QRACs, but also outlining some other potential applications. Finally, in Section 7, I consider two foundational issues connected to the nUB construction: the geometry of quantum states, and the question of genuine $n$-th order interference.

## 2 Quantum random access codes

The short description of an $n^d \rightarrow 1$ quantum random access code (QRAC) is as follows (see Fig. 1). Alice is given a classical input $x = \{x_1, x_2, \ldots, x_n\}$, which is a string of dits, i.e. $x_i \in [d]$, where I use the notation $[d] = \{1, 2, \ldots, d\}$. Alice then is allowed to send one $d$-dimensional (quantum) state to Bob, denoted by $\rho_x$, depending on her input. Bob is given a classical input $y \in [n]$, and his task is to guess $x_y$. Generally, he makes his guess by performing a measurement $M^y$ on the state, depending on his input, where $M^y = \{M^y_b\}_{b=1}^d$. The measurement satisfies the usual conditions: $\sum_{b=1}^d M^y_b = 1$ and $M^y_b \geq 0$. The usual question is: what states and measurements give the optimal strategy for a QRAC? By optimality, in the following, I mean maximal average success probability (ASP):

$$\bar{p} = \frac{1}{nd^n} \sum_{x,y} \mathbb{P}(B = x_y | X = x, Y = y) = \frac{1}{nd^n} \sum_{x,y} \text{tr}(\rho_x M^y_{x_y}),$$  \hspace{1cm} (1)$$

where the capital letters denote the probabilistic variables of the corresponding lower-case symbols, and $x$ and $y$ run along all their possible values (I implicitly assume uniform distribution on the inputs, see [19]).

Some cases are already well-studied [13], and it is proven that in the $n = 2$ case, mutually unbiased measurements (or, more abstractly, mutually unbiased bases, MUBs) give the optimal strategy. This can always be done, since there exists a pair of MUBs in any dimension. For the readers’ convenience, I recall the definition of MUBs.
Definition 2.1. Consider two orthogonal bases on $\mathbb{C}^d$, $\{|y_i\rangle\}_{i=1}^d$ and $\{|z_j\rangle\}_{j=1}^d$. We say that these bases are mutually unbiased, if they satisfy
\[ |\langle y_i | z_j \rangle| = \frac{1}{\sqrt{d}} \quad \forall i, j \in [d]. \tag{2} \]

Using this definition, the following theorem is proven in [18]:

**Theorem 2.2.** For a $2^d \rightarrow 1$ QRAC, the optimal strategy is obtained by measuring in MUBs of dimension $d$.

## 3 $n$-fold unbiased bases

In the following, using a similar line of argument with which it’s proven that MUBs are optimal for $2^d \rightarrow 1$ QRACs, I will show that a natural generalization of these bases provide optimal strategies for $n^d \rightarrow 1$ QRACs. Let me give the definition of the mentioned generalization. Later on, I will show that this condition arises naturally in the QRAC scenario.

Definition 3.1. Consider $n$ orthogonal bases on $\mathbb{C}^d$, $\{|y_{x_y}\rangle\}_{x_{y}=1}^d$, where $y = 1, \ldots, n$. We say that these bases are $n$-fold unbiased, if they satisfy
\[ \sum_{\sigma \in S_n} \prod_{y=1}^n (\langle y_{x_y} | \sigma(y) \rangle)_{x_{\sigma(y)}} = \frac{(n-1)!}{d^{n-1}} \quad \forall x_1, \ldots, x_n \in [d]. \tag{3} \]

Remark. Here $\sigma$ is an element of the permutation group $S_n$. Note that the essence of this criterion is that these terms should be uniform for each $x_1, \ldots, x_n \in [d]$. The particular value comes from the restriction when we sum up over all $x_1, \ldots, x_n$, and that there are $(n-1)!$ $n$-cycles in $S_n$. Also note, that for $n = 2$, we get the MUB condition, Eq. (2).

Now, my main result concerning QRAC strategies is the following:

**Theorem 3.2.** For an $n^d \rightarrow 1$ QRAC with $d \geq n$, the optimal strategy is obtained by measuring in $n$U Bs of dimension $d$.

In the next section, I provide the methods for proving the above theorem.
4 Methods

In order to prove the main theorem, several results are needed on QRAC strategies. The following lemmas allow us to only use pure states on both the encoding and the decoding sides:

Lemma 4.1. For an $n^d \rightarrow 1$ QRAC, pure state encoding is sufficient to reach an optimal strategy.

Proof. See [19].

This means, that in fact $\rho_x = |\psi_x\rangle \langle \psi_x|$, a pure state on $\mathbb{C}^d$. Next, it is shown in [34], that von Neumann measurements are optimal.

Lemma 4.2. For an $n^d \rightarrow 1$ QRAC, von Neumann measurements are sufficient to reach an optimal strategy.

Proof. See [34].

Which means, that in fact, $\{ |y^b\rangle \}^b_y = \{ |y^b\rangle \}^b_y$, where $|y^b\rangle \in \mathbb{C}^d$ and $\sum_y |y^b\rangle \langle y^b| = 1$ for each $b$.

It is then rather straightforward, and shown in [18], that for any set of measurements on Bob’s side, the optimal encoding for an input $x$ is the eigenvector $|\psi^x\rangle$ of the operator

$$M_x = \sum_y |y^x\rangle \langle y^x|,$$

that corresponds to the largest eigenvalue $\lambda^\text{max}_x$. The ASP then becomes

$$\bar{p} = \frac{1}{nd^n} \sum_x \lambda^\text{max}_x.$$  (5)

The task is to maximize this expression by choosing optimal measurements. I will concentrate on the characteristic polynomial of $M_x$, since its zeroes give (among other eigenvalues) $\lambda^\text{max}_x$. First, note that if $d \geq n$, in the optimal case we can assume that the vectors $\{ |y^x\rangle \}^y_x$ span an $n$-dimensional subspace in $\mathbb{C}^d$ for every $x$. This is because otherwise the optimization for every $x$ is restricted to a lower dimensional subspace, giving in general suboptimal results. We can then consider this set of vectors a (not necessarily orthogonal) basis for this subspace, and write the matrix of $M_x$ in this basis. It is easy to see that this will be the Gramian matrix of the set $\{ |y^x\rangle \}^y_x$, i.e. in this basis, $(M_x)_{yy'} = \langle y^x_x|y'^x_x\rangle$. For now, I will suppress the index $x$ for notational simplicity, and analyse the eigenvalue $\lambda^\text{max}$ of the operator $M = \sum_y |y\rangle \langle y|$.

The characteristic polynomial in general takes the form

$$P(\lambda) = \lambda^n + c_1 \lambda^{n-1} + c_2 \lambda^{n-2} + \cdots + c_n,$$  (6)

where the coefficients $c_k$ can be written as

$$c_k = (-1)^k \sum_{|J|=k} M[J],$$  (7)

where $M[J]$ is the principal minor of the matrix $M$, that corresponds to the set $J \subseteq \{1, \ldots, n\}$. So, for example, $c_1 = -\text{tr} M$ and $c_n = (-1)^n \det M$.

The following lemma is crucial in obtaining the optimal measurement bases:
Lemma 4.3. The maximal eigenvalue $\lambda^{\text{max}}$ of the operator $M = \sum_y |y\rangle \langle y|$ is a concave function of all the coefficients $c_k$ in the characteristic polynomial, expressed by Eq. (7).

Proof. First, analyse the characteristic polynomial, now only as a function of $c_k$, assuming all other coefficients to be constant. (Note that by varying $c_k$, in reality, we’re altering all other $c_l$ coefficients, as we are altering the measurement bases. For now, I forget about this fact, and am looking for purely the best solution based on a generic characteristic polynomial):

$$P_{c_k} (\lambda) = \lambda^n + c_1 \lambda^{n-1} + c_2 \lambda^{n-2} + \cdots + c_n. \quad (8)$$

It depends linearly on all coefficients $c_k$, thus any series expansion is of first order:

$$P_{c_k + dc_k} (\lambda) = P_{c_k} (\lambda) + \lambda^{n-k} dc_k, \quad (9)$$

where $dc_k$ is an infinitesimal change in $c_k$. Let’s now call $\lambda^{\text{max}}$ the maximal zero of this modified polynomial, i.e. $P_{c_k + dc_k} (\lambda^{\text{max}}) = 0$, whereas $P_{c_k} (\lambda^{\text{max}}) = 0$ from the original problem. I am interested in the concavity of $\lambda^{\text{max}}$ in $c_k$, i.e. the sign of the second derivative $\frac{\partial^2 \lambda^{\text{max}}}{\partial c_k^2}$. For this, expand $\lambda^{\text{max}}$ up to second order:

$$\lambda^{\text{max}} = \lambda^{\text{max}} + d\lambda^{\text{max}} = \lambda^{\text{max}} + \frac{\partial \lambda^{\text{max}}}{\partial c_k} dc_k + \frac{1}{2} \frac{\partial^2 \lambda^{\text{max}}}{\partial c_k^2} dc_k^2 + O(dc_k^3). \quad (10)$$

Also, expand $P_{c_k} (\lambda)$ in $\lambda$ to second order, around $\lambda^{\text{max}}$:

$$P_{c_k} (\lambda^{\text{max}}) = P_{c_k} (\lambda^{\text{max}}) + \frac{\partial P}{\partial \lambda} \bigg|_{c_k, \lambda^{\text{max}}} d\lambda^{\text{max}} + \frac{\partial^2 P}{\partial \lambda^2} \bigg|_{c_k, \lambda^{\text{max}}} (d\lambda^{\text{max}})^2$$

$$= \frac{\partial P}{\partial \lambda} \bigg|_{c_k, \lambda^{\text{max}}} d\lambda^{\text{max}} + \frac{\partial^2 P}{\partial \lambda^2} \bigg|_{c_k, \lambda^{\text{max}}} (d\lambda^{\text{max}})^2, \quad (11)$$

as the first term vanishes. Now, evaluate Eq. (9) at $\lambda^{\text{max}}$ up to second order, using Eqs. (10) and (11):

$$0 = \frac{\partial P}{\partial \lambda} \bigg|_{c_k, \lambda^{\text{max}}} \left( \frac{\partial \lambda^{\text{max}}}{\partial c_k} dc_k + \frac{1}{2} \frac{\partial^2 \lambda^{\text{max}}}{\partial c_k^2} dc_k^2 \right) + \frac{1}{2} \frac{\partial^2 P}{\partial \lambda^2} \bigg|_{c_k, \lambda^{\text{max}}} \left( \frac{\partial \lambda^{\text{max}}}{\partial c_k} \right)^2 dc_k^2$$

$$+ (\lambda^{\text{max}})^{n-k} dc_k. \quad (12)$$

Since $dc_k$ is an arbitrary infinitesimal, the terms multiplying $dc_k$ and $dc_k^2$ should be equal independently, yielding the following two equations, respectively:

$$\frac{\partial P}{\partial \lambda} \bigg|_{c_k, \lambda^{\text{max}}} \frac{\partial \lambda^{\text{max}}}{\partial c_k} = -(\lambda^{\text{max}})^{n-k} \quad (13)$$

$$\frac{\partial^2 P}{\partial \lambda^2} \bigg|_{c_k, \lambda^{\text{max}}} \frac{\partial \lambda^{\text{max}}}{\partial c_k} = -\frac{\partial^2 P}{\partial \lambda^2} \bigg|_{c_k, \lambda^{\text{max}}} \left( \frac{\partial \lambda^{\text{max}}}{\partial c_k} \right)^2. \quad (14)$$

Then, analyse the derivatives of $P(\lambda)$ at $\lambda^{\text{max}}$. Remember, that $P(\lambda)$ is the characteristic polynomial of the operator $M$ in Eq. (4), which is positive. This
means that all its eigenvalues (i.e. the zeroes of $P(\lambda)$) are real positive numbers. Then, invoke the Gauss–Lucas theorem (see e.g. [35, Theorem 6.1]), that says that for a polynomial $P(\lambda)$, all the zeroes of $\frac{\partial P}{\partial \lambda}$ belong to the convex hull of the set of zeroes of $P$. For us, this means that none of the derivatives $\frac{\partial P}{\partial \lambda}$ and $\frac{\partial^2 P}{\partial \lambda^2}$ change signs outside of the region $[\lambda_{\min}, \lambda_{\max}]$. It is clear from Eq. (8) that both of these derivatives are positive in the limit $\lambda \to \infty$. For the moment, let’s assume that $\lambda_{\max}$ is a nondegenerate zero of $P$. Then it follows that both $\frac{\partial P}{\partial \lambda}|_{c_k,\lambda_{\max}}$ and $\frac{\partial^2 P}{\partial \lambda^2}|_{c_k,\lambda_{\max}}$ are strictly positive. Using this in Eq. (14), it follows that $\frac{\partial^2 \lambda_{\max}}{\partial c_k^2} < 0$, proving the lemma.

In the case where $\lambda_{\max}$ is a degenerate zero of $P$, we need to investigate also Eq. (13). The RHS is always negative, while $\frac{\partial P}{\partial \lambda}|_{c_k,\lambda_{\max}}$ is positive in the non-degenerate case. In the degenerate case it is 0, and the right and left derivatives could differ in the sense that they could be equal to $0^+$ or $0^-$ (limiting from above or below). This means that the derivative $\frac{\partial^2 P}{\partial \lambda^2}$ equals $\pm \infty$. Since we are dealing with a polynomial and its zeroes, every function appearing is smooth. Thus, when approaching the degenerate case by varying $c_k$, the derivative of $\lambda_{\max}$ cannot suddenly change from a negative value to $+\infty$. Hence, we can conclude that it equals $-\infty$, and the derivative $\frac{\partial^2 P}{\partial \lambda^2}|_{c_k,\lambda_{\max}}$ that should be considered is the right derivative, which is always positive. The same observations hold for Eq. (14), and we can conclude that $\frac{\partial^2 \lambda_{\max}}{\partial c_k^2}$ is negative in the degenerate case as well.

Now, I re-introduce the index $x$, and write the maximal eigenvalue for a given $x$ as a function of the coefficients in the corresponding characteristic polynomial: $\lambda_{x,\max}(c_1)_x, (c_2)_x, \ldots, (c_n)_x)$. Then, we can write the ASP (Eq. (5)), as a function of the vectors $c_k$, that contain $(c_k)_x$ for all $x$:

$$p(c_1, c_2, \ldots, c_n) = \frac{1}{nd^n} \sum_{x} \lambda_{x,\max}(c_1)_x, (c_2)_x, \ldots, (c_n)_x).$$

The following lemma is very useful to characterize the behaviour of the ASP as a function of the vectors $c_k$:

**Lemma 4.4.** Consider the operators $M_x$ described by Eq. (4), and the corresponding coefficients $(c_k)_x$ in the characteristic polynomial, as in Eq. (7). Then for every $k$, the sum of $(c_k)_x$ over all $x$ is a constant dependent only on the dimension.

*Proof.* From Eq. (4) it is enough to show the statement for principal minors of the $M_x$ operators. I.e. let me fix $J \subseteq \{1, \ldots, n\}$, $|J| = k$, and show that $\sum_J M_x[J]$ is a constant, only depending on $d$. $M_x[J]$ is the Gram determinant of the vectors $\{|y_{x_j}, y_{x_k}\}_{y \in J}$, thus it can be written as

$$M_x[J] = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{y \in J} \langle y_{x_\sigma^{-1}y}, |\sigma(y)\rangle_{x_\sigma(y)} \rangle, \quad (16)$$

where $\sigma$ runs over all permutations on $J$. Every permutation $\sigma$ can be decomposed to disjoint cycles $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$ on the disjoint sets $J_1, J_2, \ldots, J_r \subseteq J$
and \( \cup_{i=1}^{r} J_i = J \). Then the above expression becomes:

\[
M_x[J] = \sum_{\sigma \in S_k} \text{sgn}(\sigma) \prod_{y \in J_1} \langle y_x \sigma | \sigma_1(y) \rangle \prod_{y \in J_2} \langle y_x \sigma | \sigma_2(y) \rangle \cdots \prod_{y \in J_r} \langle y_x \sigma | \sigma_r(y) \rangle.
\]  

(17)

When we sum up over \( x \), it is equivalent to saying that we sum up over all \( x_y \). Hence in the above expression, we can evaluate the sum over \( x \) independently on each product over \( y \in J_i \), summing up over all \( x_y \) such that \( y \in J_i \). Then, for proving the lemma, I have to show that all expressions of the form

\[
m_i = \sum_{x_y : y \in J_i} \prod_{y \in J_i} \langle y_x \sigma_1(y) \rangle
\]

(18)

are constant, depending only on \( d \). Let’s say that \( \sigma_i \) is a \( k_i \)-cycle. Clearly, if \( k_i = 1 \), then \( m_i = d \). Now, for \( k_i > 1 \), we can always order the product in a way that the ket and bra of the same \( y_{x_y} \) appear next to each other. Explicitly, it means that with this ordering:

\[
m_i = \sum_{x_y : y \in J_i} \langle y_{x_y} | \sigma_i(y_{x_y}) \rangle \langle \sigma_i(y_{x_y}) | \sigma_1^2(y_{x_y}) \rangle \langle \sigma_1^2(y_{x_y}) | \cdots | \sigma_r^2(y_{x_y}) \rangle,
\]

(19)

for some arbitrary \( y^* \in J_i \). Now, when summing up over any \( x_y \) such that \( y \neq y^* \), we get that \( \sum_{x_y} |y_{x_y}\rangle \langle y_{x_y}| = 1 \) from the orthonormality of the measurement bases. Thus

\[
m_i = \sum_{x_y : y = y^*} \langle y_{x_y} | y_{x_y}^* \rangle = d,
\]

(20)

and the proof is complete. \( \square \)

It is also important to note that since \( M_x \) is positive, all its prinicipal minors are positive. This means, that the sign of \( \langle c_i | x \rangle \) is \((-1)^k\) for all \( x \). This, together with Lemma 4.4, means that we can look at the vectors \( c_i \) as probability distributions normalized to some constants that depend only on the dimension. Thus, the ASP in Eq. (15) is a function on probability distributions, and from Lemma 4.3, it follows that it is a Schur-concave function of all the vectors \( c_1, c_2, \ldots, c_n \). [36, Theorems A.3, A.4]. But then it follows that it is maximized by all such distributions set uniform [36, Proposition B.2.].

Now, let’s discuss what does the uniformity of these vectors mean. If we follow the argument in the proof of Lemma 4.4, we see that the only terms that appear in \( c_k \), but are not present in any \( c_l \) with \( l < k \) are

\[
\sum_{\sigma \in S_k} \prod_{y \in J} \langle y_{x_y} | \sigma(y_{x_y}) \rangle =: k \text{UB}_x[J],
\]

(21)

for all \( J \subseteq \{1, \ldots, n\} \), \( |J| = k \) (this is because if \( \sigma \) is not a \( k \)-cycle, it can be decomposed to disjoint \( l < k \) cycles, and the terms we obtain from this decomposition have already appeared in \( c_l \)). Thus, if all \( c_l \) with \( l < k \) are uniform, the only task left is to set \( k \text{UB}_x[J] \) uniform for all \( x \). Similarly, as in the proof of Lemma 4.4, we see that this uniform value is

\[
k \text{UB}_x[J] = \frac{(k - 1)!}{d^{k-1}} \quad \forall x_{y_1}, \ldots, x_{y_k} \in [d], \quad y_1, \ldots, y_k \in J
\]

(22)
for all $J \subseteq \{1, \ldots, n\}$, $|J| = k$. This is because $a$) there are $(k - 1)!$ $k$-cycles in $S_{k_n}$ as we saw in Lemma 4.4 $\sum_{x \in J} \prod_{y \in J} \langle y_{x_y} | \sigma(y)_{x_{\sigma(y)}} \rangle = d$ if $\sigma$ is a $k$-cycle, and $c$) there are $d^k$ different $k$UB at all for all possible $x_{y_1}, \ldots, x_{y_k} \in [d]$. At this point, I note that it should not be necessary to set the same values for all the possible $J$ subsets, but eventually it will turn out that this should be the case. I also refer the reader to Definition 3.1 from where it’s clear that the index $k$ of our measurement bases should form a $k$UB. The following theorem on $n$UBs simplifies the criteria on optimal QRAC measurements, and finalize the proof of Theorem 3.2.

**Theorem 4.5.** If $n$ orthonormal bases form an nUB, then any subset of $n - 1$ bases forms an $(n - 1)$UB.

**Proof.** Remember that the $n$ bases $\{|y_{x_y}\rangle\}_{x_y=1}^d$ for $y = 1, \ldots, n$ form an $n$UB iff

$$\sum_{\sigma \in S_n} \prod_{y=1}^n \langle y_{x_y} | \sigma(y)_{x_{\sigma(y)}} \rangle = \frac{(n-1)!}{d^{n-1}} \quad \forall x_1, \ldots, x_n \in [d]. \quad (23)$$

Pick an arbitrary subset of $n - 1$ bases by omitting one basis, say $\{|k_{x_k}\rangle\}_{x_k=1}^d$, for some $k \in \{1, \ldots, n\}$. Now, sum up Eq. (23) over the index $x_k$. This, as we saw in the proof of Lemma 4.4, eliminates the term $|k_{x_k}\rangle \langle k_{x_k}|$ from each term to the summand, as $\sum_{x_k} |k_{x_k}\rangle \langle k_{x_k}| = 1$. The summation on the RHS of Eq. (23) clearly yields $\frac{(n-1)!}{d^{n-2}}$, thus the equation now reads as:

$$\sum_{\sigma \in S_n} \prod_{y=1}^n \langle y_{x_y} | \sigma(y)_{x_{\sigma(y)}} \rangle = \frac{(n-1)!}{d^{n-2}} \quad \forall \{x_1, \ldots, x_n\} \setminus \{x_k\} \in [d]. \quad (24)$$

We can write the LHS of the above equation (reordering the product to a desirable form) as:

$$\sum_{\sigma \in S_n} \langle \sigma(k)_{x_{\sigma(k)}} | \sigma^2(k)_{x_{\sigma^2(k)}} \rangle \langle \sigma^2(k)_{x_{\sigma^2(k)}} | \cdots | \sigma^{n-1}(k)_{x_{\sigma^{n-1}(k)}} \rangle \langle \sigma^{n-1}(k)_{x_{\sigma^{n-1}(k)}} | \sigma(k)_{x_{\sigma(k)}} \rangle. \quad (25)$$

The permutation $\sigma$ can be represented by the chain of elements, up to a cyclic permutation as $\sigma = [\sigma(k), \sigma^2(k), \ldots, \sigma^{n-1}(k), k]$. (26)

Note that in Eq. (25), we only use the first $n - 1$ elements of this representation, since the index $k$ is not present anymore. In fact, for our purposes, we can look at the first $n - 1$ elements as an artificial $(n - 1)$-cycle $\sigma_1$, and write Eq. (25) as

$$\sum_{\sigma \in S_n} \prod_{y=1}^n \langle y_{x_y} | \sigma_1(y)_{x_{\sigma_1(y)}} \rangle. \quad (27)$$

Nevertheless, the summation still runs along all the $(n - 1)!$ $n$-cycles, and not the new $(n - 1)$-cycles. What is the connection between these? Let’s consider new
n-cycles \( \sigma \), by cyclically permuting the first \( n - 1 \) elements in the representation Eq. (26) of \( \sigma \):

\[
\sigma = [\pi(\sigma(k)), \pi(\sigma^2(k)), \ldots, \pi(\sigma^{n-1}(k))],
\]

(28)

where \( \pi \) is a cyclic permutation of the elements \( \sigma(k), \sigma^2(k), \ldots, \sigma^{n-1}(k) \). There are \( n - 1 \) different such \( \sigma \) permutations, each of which giving a new \( n \)-cycle. Nevertheless, \( \sigma \equiv \sigma \), the artificial \( (n-1) \)-cycles given by their first \( n - 1 \) elements are all the same, since they are only cyclic permutations of each other. Thus, when summing up over all \( n \)-cycles in Eq. (27), we use each \( (n-1) \)-cycle \( n - 1 \) times, and hence we can write it as

\[
(n - 1) \sum_{\sigma \in S_{n-1}} \prod_{y=1}^{n} \langle y_{xy} | \sigma(y)x_{\sigma(y)} \rangle,
\]

(29)

and comparing this with Eq. (24) we see that

\[
\sum_{\sigma \in S_{(n-1)}} \prod_{y=1}^{n} \langle y_{xy} | \sigma(y)x_{\sigma(y)} \rangle = \frac{(n-2)!}{d^{n-2}} \forall \{x_1, \ldots, x_n\} \setminus \{x_k\} \in [d],
\]

(30)

i.e. the set \( \{\langle y_{xy}, y \rangle \}_{y=1}^{d} \) for \( y \in \{1, \ldots, n\} \setminus \{k\} \) forms an \( (n-1) \)-UB.

Remark. Note that Theorem 4.5 implies that for an optimal \( n^d \rightarrow 1 \) QRAC strategy it is enough to have \( n \)-UB measurement bases, since the \( n \)-UB condition implies the uniformity of \( c_k \), and in fact the uniformity of all \( c_k \). Thus, the proof of Theorem 3.2 is complete.

5 Existence of \( n \)-fold unbiased bases

So far, I only established a theoretical optimum for QRAC strategies. But naturally the question arises: do these optimal measurement bases exist for any dimension? In the \( 2^d \rightarrow 1 \) case, we are always provided with a pair of MUBs in any dimension. It will turn out that this is not the case with \( n \)-UBs in general, although their existence problem is still unsolved.

5.1 Low dimensions

Theorem 4.5 provides a useful tool for searching for \( n \)-UBs. It implies that any subset of size \( n - 1 \) of a set of \( n \)-UBs should also form an \( (n-1) \)-UB, and thus eventually they should all form MUBs. MUBs are excessively studied in the quantum information community (see [10, 11]), hence making the search for \( n \)-UBs more tractable.

The easiest non-trivial search is for 3UBs. Following the above argument, every 3UB should be a triplet of MUBs. All the triplets are fully characterised in dimensions 2, 3, 4 and 5, allowing for an exhaustive search [11]. For the readers’ convenience, let me recall a set of equivalence transformations on MUBs [11, Appendix A], which are easily seen equivalence transformations also on \( n \)-UBs for any \( n \):
Definition 5.1. Consider a set of $r$ MUBs ($n$UBs) described by complex matrices $B_i$, $i = 1, \ldots, r$ of size $d \times d$, that is, the elements of basis $i$ are the columns of $B_i$. Two such lists are equivalent to each other, if they can be transformed into each other by a succession of the following five transformations:

1. an overall unitary transofmation $U$ applied from the left,

$$\{B_1, \ldots, B_r\} \rightarrow U\{B_1, \ldots, B_r\}, \quad (31)$$

which leaves invariant all the scalar products.

2. $r$ diagonal unitary transformations $D_i$ from the right which attach phase factors to each column of the $r$ matrices,

$$\{B_1, \ldots, B_r\} \rightarrow \{B_1 D_1, \ldots, B_r D_r\}. \quad (32)$$

This exploits the fact that the overall phase of a quantum state drops out from the conditions of MUBs ($n$UBs).

3. $r$ permutations of the elements within each basis,

$$\{B_1, \ldots, B_r\} \rightarrow \{B_1 P_1, \ldots, B_r P_r\}, \quad (33)$$

which is simply just relabeling basis elements. Here $P_i$ are unitary permutation matrices, $P_i P_i^T = 1$.

4. pairwise exchange of two bases,

$$\{\ldots, B_i, \ldots, B_j, \ldots\} \rightarrow \{\ldots, B_j, \ldots, B_i, \ldots\}. \quad (34)$$

whish is simply relabeling the bases.

5. an overall complex conjugation

$$\{B_1, \ldots, B_r\} \rightarrow \{\bar{B}_1, \ldots, \bar{B}_r\}, \quad (35)$$

which leaves invariant all the scalar products.

All equivalence classes or MUB triplets are known in dimensions 2, 3, 4 and 5. After checking these triplets for the 3UB condition, I got the following results:

In dimension 2, there is only one equivalence class of MUB triplets, which also forms a 3UB. A representative of this class is:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right\}. \quad (36)$$

Although this is promising, observe that the existence of 3UBs in dimension 2 is trivial in some sense. We already know that there exist 3 MUBs. Then, using them, in the characteristic polynomial \[3\], the uniformity of $c_3$ gives the 3UB condition. But this is the determinant of the Gramian matrix of 3 vectors for each $x$. These vectors must be linearly dependent in dimension 2, and we know that in this case, the Gram determinant is zero (see e.g. \[37\] Theorem 7.2.10]). Thus, the coefficients ($c_3$) are uniform for every $x$ (zero, in fact). Also note, that this set of 3UBs is not useful in the QRAC game, as my argument only works for $d \geq n$. Nevertheless, these measurement bases give the optimal strategy for the $3^2 \rightarrow 1$ QRAC \[19\]. The above observations can be generalized to the following result on $n$UBs:
Proposition 5.2. If there exist $d + 1$ dUBs in dimension $d$, then they also form a $(d + 1)$UB.

Proof. Assuming that the $d + 1$ bases are dUBs, in the coefficients $(c_{d+1})_x$, all the terms are uniform, except for the $(d + 1)$UB term. But $(c_{d+1})_x$ is a Gram determinant of $d + 1$ vectors in dimension $d$, thus equals zero for every $x$.

Remark. It is known that in dimension $d$, the maximal number of MUBs is $d + 1$. Also note that if $d > 2$, the dUB conditions on a set of $d + 1$ bases are more restrictive than the MUB conditions. It is then unlikely that in any dimension greater than 2, there exist $d + 1$ dUBs, and thus Proposition 5.2 may practically only be useful in the $d = 2$ case.

Since there are no more than 3 MUBs in dimension 2, there cannot exist $n$UBs with $n \geq 4$.

In dimension 3, there is also only one equivalence class of MUB triplets. If we check for the 3UB condition, it does not satisfy it, meaning that there are no $n$UBs in dimension 3 for $n \geq 3$.

In dimension 4, there is a three-parameter family of MUB triplets. Nevertheless, it turns out that they do not satisfy the 3UB condition for any value of these parameters, thus concluding that there are no $n$UBs in dimension 4 for $n \geq 3$.

In dimension 5, there are two equivalence classes of MUB triplets, none of them satisfying the 3UB condition, meaning that also in dimension 5, there are no $n$UBs for $n \geq 3$.

### 5.2 High dimensions, probabilistic arguments

In dimensions higher than 5, not all the equivalence classes of MUB triplets are known. There are some explicit constructions in prime and prime power dimensions for obtaining a full set of $d + 1$ MUBs, from which we can test arbitrary subsets for the $n$UB conditions. In composite dimensions that are not powers of primes, even the maximal number of MUBs is unknown. The lowest such dimension, 6 is excessively studied, pointing to a direction that there exist only 3 MUBs [12, 13, 16, 17].

In dimension six, I checked a one-parameter family of MUB triplets [14], which lead to no success. Apart from that, I checked some known constructions for dimensions 7, 8 and 9 [10, 38], also without any success. Nevertheless, these searches weren’t exhaustive, given the fact that there is no characterization of all the equivalence classes of MUB triplets in these dimensions.

The situation thus seems a little desperate at this point. On the bright side, when we move to high dimensions, there are some probabilistic arguments supporting the possibility of existence of $n$UBs. Consider $n$ uniformly random states on $\mathbb{C}^d$, constructed as follows: fix a state $|x_1\rangle$ in the computational basis. Then draw unitaries $U_2, U_3, \ldots, U_n$ uniformly and independently with respect to the Haar measure on $U_d$, and apply it to the other states of the computational basis: $U_y|x_y\rangle$ with $y = 2, 3, \ldots, n$. We will be interested in the expectation value of the $n$UB expression Eq. (3) for these states, with the correspondence $|y_{x_y}\rangle := U_y|x_y\rangle$:

$$
E\left( \sum_{\sigma \in S_n} \prod_{y=1}^{n} \langle x_y|U_y^{\sigma(y)}x_{\sigma(y)}\rangle \right),
$$

(37)
where the expectation value is over \( \cup_d \) with the Haar measure, and we say that \( U_1 = 1 \).

Since the expectation value is linear, we can concentrate on one term in the above sum. Pick the term with \( \sigma = [1, 2, \ldots, n] \), and write out the expectation value:

\[
\mathbb{E}
\left[
\langle x_1|U_2|x_2\rangle \langle x_2|U_3^d|x_3\rangle \langle x_3|U_3^d\cdots U_n^d|x_n\rangle \langle x_n|U_n^d|x_1\rangle
\right]
\]

\[
= \mathbb{E}
\left[
\langle x_1|U_2|x_2\rangle \langle x_2|U_2^d \sum_{k_2=1}^d |k_2\rangle \langle k_2|U_3|x_3\rangle \langle x_3|U_3^d \sum_{k_3=1}^d |k_3\rangle \cdots \right.
\]

\[
\sum_{k_{n-1}=1}^d |k_{n-1}\rangle \langle k_{n-1}|U_n|x_n\rangle \langle x_n|U_n^d|x_1\rangle
\]

\[= \sum_{k_2,k_3,\ldots,k_{n-1}=1}^d \mathbb{E}
\left[
\langle x_1|U_2|x_2\rangle \langle x_2|U_2^d|k_2\rangle \langle k_2|U_3|x_3\rangle \langle x_3|U_3^d|k_3\rangle \cdots \right.
\]

\[
\sum_{k_{n-1}=1}^d \mathbb{E}
\left[
\langle k_{n-1}|U_n|x_n\rangle \langle x_n|U_n^d|x_1\rangle
\right]
\]

inserting identities in between the different unitaries in the first equality, and using the linearity of the expectation value and the fact that the unitaries are independently drawn, in the second one. Now, let’s calculate in general the above expectation values:

\[
\mathbb{E}
\left[
\langle x_i|U_y|x_y\rangle \langle x_y|U_n^d|x_j\rangle
\right]
\]

\[
= \int \langle x_i|U|x_y\rangle \langle x_y|U^d|x_j\rangle dU = \langle x_i|\left( \int U|x_y\rangle \langle x_y|U^d\right) dU|x_j\rangle
\]

\[
= \langle x_i|\frac{1}{d}|x_j\rangle = \frac{1}{d} \delta_{ij}
\]

(39)

where \( dU \) is the Haar measure, and the linearity of the inner product is used. Plugging this into Eq. (38), we get that

\[
\mathbb{E}
\left[
\langle x_1|U_2|x_2\rangle \langle x_2|U_2^d U_3|x_3\rangle \langle x_3|U_3^d U_4\cdots U_{n-1}^d U_n|x_n\rangle \langle x_n|U_n^d|x_1\rangle
\right]
\]

\[
= \sum_{k_2,k_3,\ldots,k_{n-1}=1}^d \frac{1}{d^{n-1}} \langle x_1|k_2\rangle \langle k_2|k_3\rangle \cdots |k_{n-1}\rangle \langle k_{n-1}|x_1\rangle = \frac{1}{d^{n-1}}
\]

(40)

and observe that for any \( \sigma \) \( n \)-cycle, we get the same value. Thus, we can conclude, that

\[
\mathbb{E}
\left[
\sum_{\sigma \in S_n} \prod_{y=1}^n \langle x_y|U_y^d U_{\sigma(y)}|x_{\sigma(y)}\rangle
\right]
\]

\[
= \frac{(n-1)!}{d^{n-1}}
\]

(41)

This means that the expectation value of the \( n \)UB expression for \( n \) independent, uniformly random states is exactly the \( n \)UB condition. This is promising, as it implies that a set of states forming \( n \)UBs could even be something typical.

In general, one would then prove existence by using the probabilistic method [39], thus invoking concentration of measure, in particular, Lévy’s lemma (see e.g. [40] Theorem 4) or [41]:
Lemma 5.3 (Lévy’s lemma). Let $f : S^{2d-1} \rightarrow \mathbb{R}$ be Lipschitz-continuous with Lipschitz constant $\eta$, i.e.

$$|f(x) - f(y)| \leq \eta \cdot \|x - y\|,$$  \hspace{1cm} (42)

where $\|\cdot\|$ is the Euclidean norm on $\mathbb{R}^{2d}$. Then, drawing a point $x \in S^{2d-1}$ randomly with respect to the uniform measure on the sphere yields

$$\mathbb{P}(|f(x) - \mathbb{E}f| \geq \epsilon) \leq 2 \exp\left(\frac{d\epsilon^2}{9\pi^3\eta^2}\right)$$  \hspace{1cm} (43)

for all $\epsilon \geq 0$.

This means that for a real-valued function on pure states of dimension $d$, the probability of deviating from its expectation value decreases exponentially with increasing dimension, provided an appropriate Lipschitz constant.

The function on $d$-dimensional pure states, whose expectation value are calculated in Eq. (39) is $f_{ij} : |\psi\rangle \rightarrow \langle x_i|\psi\rangle \langle \psi|x_j\rangle$. Now, even though its expectation value is real, in general it is not a real-valued function, thus the above lemma does not apply. Also, if one wants to see uniformity of the expression $n_{UB}$ for all $x$, the states are not independent anymore, as certain subsets have to form orthogonal bases.

To sum it up, the fact that the expectation value of the $n_{UB}$ expression is what we want it to be is promising. Although, to prove existence, the usual probabilistic method faces difficulties. Some more refined concentration of measure results on complex valued functions, or functions on unitaries would be needed, if one wanted to prove existence this way.

6 Applications

In this section, I give a few (potential) applications of the above defined bases. We certainly know a lot about their implications on QRAC strategies now, and I outline some possible applications on other tasks otherwise related to MUBs. Apart from the protocols mentioned here, one could consider other tasks usually discussed in the context of MUBs. Note that if the bases in question don’t exist, they still provide a bound on what can we achieve within the framework of quantum mechanics, and this bound is close-to-tight, at least in the QRAC scenario.

6.1 Upper bounds on QRAC success probabilities

Naturally, $n_{UB}$s in dimension $d$ provide optimal $n^d \rightarrow 1$ QRAC measurements, as long as $d \geq n$. In the case when they exist, this is a tight upper bound on quantum strategies. Nevertheless, in the case when they don’t exist, they still give a close-to-tight upper bound. To demonstrate this, I provide a table with the ASP of the optimal classical, the MUB and the $n_{UB}$ quantum strategies for some simple cases:
| $d$ | $n = 3$ | $n = 4$ | $n = 4$ |
|-----|---------|---------|---------|
| 3   | 0.6296  | 0.6971  | 0.6989  |
| 4   | 0.5625  | 0.6443  | 0.6466  |
| 5   | 0.5200  | 0.6109  | 0.6114  |

Here, the classical values are computed using the method of [42], the MUB values are results of straightforward calculations exploiting the known equivalence classes, and the nUB values are computed by calculating $\lambda_{\text{max}}$, assuming uniform coefficients in $x$ for every $k$ in the characteristic polynomial, Eqs. (6), (7).

On the other hand, I note that the see-saw optimization, also used in [18], results in MUB measurements for $n = 3$, in dimensions 3-7. This serves as numerical evidence for MUB optimality whenever nUBs don’t exist, and also for the non-existence of 3UBs in dimensions 6, 7. An open question remains whether MUBs provide optimal measurements for any $n^d \rightarrow 1$ QRAC protocol.

Remember that any pair of nUBs also form MUBs, thus in this sense, MUBs do provide optimal measurements for general QRACs. Although, when nUBs don’t exist in the given dimension, the question of optimal QRAC strategies becomes more difficult. To see this, consider the optimization of a $3^d \rightarrow 1$ QRAC in some dimension where 3UBs don’t exist. This means that the vector $c_3$ cannot be set uniform. On the other hand, there exist 3 MUBs in any dimension, thus $c_2$ can always be set uniform. Although, this doesn’t imply that MUBs are optimal in this case, as the ASP $\bar{p}(c_2, c_3)$ is a Schur-concave function of $c_2$ and $c_3$, but this is an independent property on the two vectors. This then only means that $\bar{p}' := \bar{p}(c'_2, c'_3) < \bar{p}$ whenever $c_2 \succ c'_2$ and $c_3 \succ c'_3$, where $\succ$ expresses majorization (see e.g. [36]). We cannot say anything about the relation of $\bar{p}'$ and $\bar{p}$, when e.g. $c_2 \succ c'_2$ and $c_3 \prec c'_3$, and one can construct bases such that these relations hold. Nevertheless, the above mentioned numerical evidence supports the optimality of MUBs for $3^d \rightarrow 1$ QRACs.

I note, as it’s pointed out in [18], that if we restrict ourselves to MUB optimization, then different equivalence classes can yield different ASPs. The simplest case is $d = 5, n = 3$, where the two inequivalent MUB triplets perform differently. This is because there don’t exist 3UBs in dimension 5, but the two equivalence classes have different 3UB properties, and the one being more uniform gives a better QRAC strategy.

Since polynomials up to order 4 are analytically solvable, the nUB method provides analytic bounds for $n^d \rightarrow 1$ QRAC ASPs for $n = 2, 3, 4$ with $d \geq n$. I note that for $n = 2$, this bound is tight and is previously found in [18]:

$$\bar{p}_{n=2} \leq \frac{1}{2} \left( 1 + \frac{1}{\sqrt{d}} \right) \quad (44)$$

$$\bar{p}_{n=3} \leq \frac{1}{3} \left( 1 + \frac{d}{2} \left( \frac{d^4 + \sqrt{d^8 - d^9}}{d} \right)^{1/3} + \left( \frac{d^4 + \sqrt{d^8 - d^9}}{d^2} \right)^{1/3} \right) \quad (45)$$

The formula for $n = 4$ is too complicated to present here, but it is the greatest
zero of the polynomial
\[
\lambda^4 - 4\lambda^3 + 6\left(1 - \frac{1}{d}\right)\lambda^2 - 4\left(1 - \frac{3}{d} + \frac{2}{d^2}\right)\lambda + 1 - \frac{6}{d} + \frac{11}{d^2} - \frac{6}{d^3},
\]
divided by 4.

If \( n > 4 \), the polynomials are not solvable analytically anymore, nevertheless, one can solve them numerically up to machine precision (e.g. by Newton’s method, with starting point \( n \)). This gives an upper bound on the given \( n^d \to 1 \) QRAC ASP. Also, if \( n \) MUBs exist in dimension \( d \), they give a lower bound. In low dimensions, these bounds are close-to-tight, and this is expected in higher dimensions as well, thus one has a good estimate on optimal QRAC ASPs for a wide class of \( n \) and \( d \).

### 6.2 Entropic uncertainty relations

Entropic uncertainty relations are a refined version of Heisenberg’s uncertainty relations (see the seminal paper of Maassen and Uffink [3], and the surveys [4][5]). Consider \( n \) observables on \( \mathbb{C}^d \), described by projections on the states \( \{ |y\rangle_x \}_{x=1}^n \), \( y \in [n] \). Then define the probabilities \( p_{y|x} = |\langle y|x\rangle|\psi\rangle|^2 \) for some \( |\psi\rangle \in \mathbb{C}^d \). The aim is then to put a lower bound on \( \sum_{y=1}^n H\{p_{y|x}\} \), where \( H \) is the Shannon entropy. It is shown in [3], that when \( n = 2 \),
\[
H\{p_{y|x}\} + H\{p_{z|x}\} \geq - \log c,
\]
where \( c = \max_{x,y,z} |\langle y|x\rangle|\psi\rangle|^2 \). This bound is independent on the state \( |\psi\rangle \), and the lowest possible value of \( c \) is attained by mutually unbiased bases, for which \( c = \frac{1}{d} \).

In the case of more than two observables, no general tight bound is known. Based on the fact that the bound for \( n = 2 \) is related to the uniformity of MUBs, I propose that \( n \) MUBs could provide potential means of exploring and understanding entropic uncertainty relations for \( n \) observables.

### 6.3 Information locking

An information theoretical task closely related to entropic uncertainty relations is that of information locking (see [6][7] for detailed description). Here, classical correlations are hidden (locked) in quantum states, until a key is revealed. It turns out that by revealing this extra information, arbitrarily large increase can be obtained in the correlations. In the simplest case, this means that one party is encoding a classical bit in a qudit, using one of two mutually unbiased bases. Sending this qudit, but not the information on the encoding basis (one bit key) to a receiver leaves them with very limited classical correlation, since measuring in the wrong basis provides no information on the encoded bit whatsoever. Sending the key, on the other hand reveals the full information, thus increases classical correlation to its maximal value.

It is known that for a one-bit key, corresponding to two possible encoding bases, mutually unbiased bases provide optimal locking properties. I propose that in the case of \( n \) possible encoding bases, \( n \) MUBs could provide close-to-tight bounds on locking tasks.
7 Foundational implications

Apart from their use in information theoretical protocols, and providing bounds on certain tasks, the question of existence of UBs raises some fundamental questions about the quantum world. One of these is solely the structure of quantum states, which we still strive to understand, especially in higher dimensions. On the other hand, considering the fact that in the QRAC scenario, UBs are extremely close to what is achievable within quantum mechanics, it is natural to ask if their existence is prohibited merely by the formulation of quantum mechanics, or is it some fundamental property of Nature. A foundational question seemingly well-fit for investigating this problem is that of the existence of genuine high-order interference in Nature.

7.1 Geometry of quantum states

While the mathematical formulation of quantum states is clear, we are struggling to characterize their geometry, especially in dimensions higher than two, where the Bloch-sphere ceases to provide an intuitive picture. Whenever we impose some conditions on certain states, such as the MUB conditions, we have an option to characterize quantum states accordingly. For instance, the long-standing question of the number MUBs in a general dimension could allow us to characterize the behaviour of quantum states in different dimensions, according to the unbiasedness one can introduce in certain protocols. In the same spirit, understanding how UBs can or cannot be constructed, could give a more general characterisation.

7.2 Genuine n-th order interference

It was noted by Sorkin [43], that quantum mechanics only exhibits second-order genuine interference. Simply saying, having a two-slit experiment with quantum particles, the interference pattern cannot be written in terms of one-slit experiments. On the other hand, already a three-slit experiment can be written in terms of one- and two-slit experiments. This follows simply from the mathematical formulation of quantum mechanics. The natural question then arises, whether Nature admits genuine higher-order interference, or if not, what is the fundamental reason behind it. It is worth to note that even if there is higher-order interference, there is experimental evidence that it is suppressed by at least a factor of $\sim 10^2$ by second-order interference [44, 45].

For studying this question, researchers have come up with theories (in general, general probabilistic theories) that exhibit genuine higher-order interference (see e.g. [46, 47], or [48] for a review on them). For now, I will focus on the theory of Density Cubes of Dakić et al. [46]. They point out that the description of quantum states by density matrices $\rho_{ij}$ inherently only allows for interference between two levels of a quantum state. To overcome this limitation, they introduce Density Cubes, that is, states described by 3-index tensors, $\rho_{ijk}$. They construct some (incomplete) bases, and show that usual quantum states form a subset of these generalized state space. Nevertheless, it is pointed out in [48] that the axioms of this theory are insufficient to uniquely characterise it.

In any case, if one considers a set of 3UBs, $\{ |x_y \rangle \}_{x_y}, \{ |z_z \rangle \}_{z_z}, \{ |a_a \rangle \}_{a_a}$,
then in the 3UB condition
\[
\langle y_{x_y} | z_{x_z} \rangle \langle z_{x_z} | a_{x_a} \rangle \langle a_{x_a} | y_{x_y} \rangle + \langle y_{x_y} | a_{x_a} \rangle \langle a_{x_a} | z_{x_z} \rangle \langle z_{x_z} | y_{x_y} \rangle = \frac{2}{d^2} \quad \forall x_y, x_z, x_a \in [d]
\] (48)
correlations of 3 “levels” appear. It is then natural to think that if 3UBs don’t exist in some dimension within the framework of quantum mechanics, some analogue might exist within the Density Cube framework. Note that the idea of Density Cubes and this analogue can be generalized to any \( n \) other than 3.

Existence of \( n \)UBs thus could be connected to the existence of \( n \)-th order interference in Nature. Then, understanding the fundamental reasons why these theories could or could not describe Nature, could lead to understanding the existence of \( n \)UBs. Or the other way around, understanding the existence problem of \( n \)UBs could lead to non-trivial statements on \( n \)-th order interference in Nature.

Acknowledgements

I would like to thank Jakub Borka/suppress la for providing calculations on general QRAC strategies, Edgar Aguilar and Richard Küng for fruitful discussions, and Piotr Mironowicz and Debashis Saha for providing numerical results on some QRAC protocols. The work is supported by the NCN grant Sonata UM O-2014/14/E/ST2/00020

References

[1] I. D. Ivo novic, “Geometrical description of quantal state det ermination,” Journal of Physics A: Mathematical and General, vol. 14, no. 12, p. 3241, 1981.

[2] W. K. Wootters and B. D. Fields, “Optimal state-determination by mutually unbiased measurements,” Annals of Physics, vol. 191, no. 2, pp. 363 – 381, 1989.

[3] H. Maassen and J. B. M. Uffink, “Generalized entropic uncertain ty relations,” Phys. Rev. Lett., vol. 60, pp. 1103–1106, Mar 1988.

[4] S. Wehner and A. Winter, “Entropic uncertainty relations – a survey,” New Journal of Physics, vol. 12, no. 2, p. 025009, 2010.

[5] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, “Entropic uncertainty relations and their applications,” Rev. Mod. Phys., vol. 89, p. 015002, Feb 2017.

[6] M. A. Ballester and S. Wehner, “Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases,” Phys. Rev. A, vol. 75, p. 022319, Feb 2007.

[7] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, “Locking classical correlations in quantum states,” Phys. Rev. Lett., vol. 92, p. 067902, Feb 2004.
[8] P. K. Aravind, “Solution to the kings problem in prime power dimensions,” *Zeitschrift für Naturforschung A*, vol. 58, no. 2-3, p. 85, 2003.

[9] B.-G. Englert and Y. Aharonov, “The mean king’s problem: prime degrees of freedom,” *Physics Letters A*, vol. 284, no. 1, pp. 1 – 5, 2001.

[10] T. Durt, B. Englert, I. Bengtsson, and K. Życzkowski, “On mutually unbiased bases,” *International Journal of Quantum Information*, vol. 8, no. 4, pp. 535–640, 2010.

[11] S. Brierley, S. Weigert, and I. Bengtsson, “All mutually unbiased bases in dimensions two to five,” *Quantum Info. Comput.*, vol. 10, pp. 803–820, Sept. 2010.

[12] G. Zauner, “Quantum designs: Foundations of a noncommutative design theory,” *International Journal of Quantum Information*, vol. 09, no. 01, pp. 445–507, 2011.

[13] M. Grassl, “On sic-povms and mubs in dimension 6.”

[14] P. Jaming, M. Matolesi, P. Móra, F. Szőllősi, and M. Weiner, “A generalized pauli problem and an infinite family of mub-triplets in dimension 6,” *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 24, p. 245305, 2009.

[15] F. Szőllősi, “Complex hadamard matrices of order 6: a four-parameter family,” *Journal of the London Mathematical Society*, vol. 85, no. 3, pp. 616–632, 2012.

[16] S. Brierley and S. Weigert, “Mutually unbiased bases and semi-definite programming,” *Journal of Physics: Conference Series*, vol. 254, no. 1, p. 012008, 2010.

[17] P. Butterley and W. Hall, “Numerical evidence for the maximum number of mutually unbiased bases in dimension six,” *Physics Letters A*, vol. 369, no. 12, pp. 5 – 8, 2007.

[18] E. A. Aguilar, J. J. Borkała, P. Mironowicz, and M. Pawłowski *In preparation*.

[19] Ozols, Maris, “Quantum random access codes with shared randomness,” Master’s thesis, 2009.

[20] S. Wiesner, “Conjugate coding,” *SIGACT News*, vol. 15, pp. 78–88, Jan. 1983.

[21] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, “Dense quantum coding and a lower bound for 1-way quantum automata,” in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, STOC ’99, (New York, NY, USA), pp. 376–383, ACM, 1999.

[22] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, “Dense quantum coding and quantum finite automata,” *J. ACM*, vol. 49, pp. 496–511, July 2002.
[23] A. Nayak, “Optimal lower bounds for quantum automata and random access codes,” in Proceedings of the 40th Annual Symposium on Foundations of Computer Science, FOCS ’99, (Washington, DC, USA), pp. 369–, IEEE Computer Society, 1999.

[24] E. F. Galvão, Foundations of quantum theory and quantum information applications. PhD thesis, Oxford Univ., Oxford, 2002. Presented on 22 Dec 2002.

[25] H. Klauck, “Lower bounds for quantum communication complexity,” in Proceedings 2001 IEEE International Conference on Cluster Computing, pp. 288–297, Oct 2001.

[26] S. Aaronson, “Limitations of quantum advice and one-way communication,” in Proceedings of the 19th IEEE Annual Conference on Computational Complexity, CCC ’04, (Washington, DC, USA), pp. 320–332, IEEE Computer Society, 2004.

[27] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf, “Bounded-error quantum state identification and exponential separations in communication complexity,” in Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing, STOC ’06, (New York, NY, USA), pp. 594–603, ACM, 2006.

[28] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “(4, 1)-quantum random access coding does not exist,” in 2006 IEEE International Symposium on Information Theory, pp. 446–450, July 2006.

[29] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, Quantum Network Coding, pp. 610–621. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[30] I. Kerenidis, Quantum Encodings and Applications to Locally Decodable Codes and Communication Complexity. PhD thesis, Berkeley, CA, USA, 2004. AAI3165439.

[31] I. Kerenidis and R. de Wolf, “Exponential lower bound for 2-query locally decodable codes via a quantum argument,” Journal of Computer and System Sciences, vol. 69, no. 3, pp. 395 – 420, 2004. Special Issue on STOC 2003.

[32] S. Wehner and R. de Wolf, Improved Lower Bounds for Locally Decodable Codes and Private Information Retrieval, pp. 1424–1436. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[33] A. Ben-Aroya, O. Regev, and R. d. Wolf, “A hypercontractive inequality for matrix-valued functions with applications to quantum computing and ldec,” in 2008 49th Annual IEEE Symposium on Foundations of Computer Science, pp. 477–486, Oct 2008.

[34] E. A. Aguilar, M. Farkas, M. Pawłowski, G. Cañas, J. Cariñe, J. F. Barra, D. Martínez, M. Alvarado, and G. Lima In preparation.
[35] M. Marden, *Geometry of Polynomials*. No. no. 3 in Geometry of Polynomials, American Mathematical Society, 1949.

[36] A. Marshall, I. Olkin, and B. Arnold, *Inequalities: Theory of Majorization and Its Applications*. Springer Series in Statistics, Springer New York, 2010.

[37] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.

[38] G. Björling and R. Fröberg, “A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots,” *Journal of Symbolic Computation*, vol. 12, no. 3, pp. 329 – 336, 1991.

[39] N. Alon and J. Spencer, *The Probabilistic Method*. Wiley Series in Discrete Mathematics and Optimization, Wiley, 2004.

[40] S. Artstein-Avidan, A. Giannopoulos, and V. Milman, *Asymptotic Geometric Analysis, Part I*. Mathematical Surveys and Monographs, American Mathematical Society, 2015.

[41] M. Gerken, “Measure concentration: Levy’s lemma,” 2013.

[42] D. Saha, M. Czechlewski, and M. Pawlowski In preparation.

[43] R. D. Sorkin, “Quantum mechanics as quantum measure theory,” *Modern Physics Letters A*, vol. 09, no. 33, pp. 3119–3127, 1994.

[44] U. Sinha, C. Couteau, T. Jennewein, R. Laflamme, and G. Weihs, “Ruling out multi-order interference in quantum mechanics,” *Science*, vol. 329, no. 5990, pp. 418–421, 2010.

[45] I. Söllner, B. Gschösser, P. Mai, B. Pressl, Z. Vörös, and G. Weihs, “Testing born’s rule in quantum mechanics for three mutually exclusive events,” *Foundations of Physics*, vol. 42, no. 6, pp. 742–751, 2012.

[46] B. Daki, T. Paterek, and . Brukner, “Density cubes and higher-order interference theories,” *New Journal of Physics*, vol. 16, no. 2, p. 023028, 2014.

[47] K. Życzkowski, “Quartic quantum theory: an extension of the standard quantum mechanics,” *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 35, p. 355302, 2008.

[48] C. M. Lee and J. H. Selby, “Higher-order interference in extensions of quantum theory,” *Foundations of Physics*, vol. 47, no. 1, pp. 89–112, 2017.