This is a repository copy of *Uncertainty relations for the support of quantum states*.

PAPER • OPEN ACCESS

Uncertainty relations for the support of quantum states

To cite this article: Vincenzo Fiorentino and Stefan Weigert 2022 *J. Phys. A: Math. Theor.* **55** 495305

View the article online for updates and enhancements.

Uncertainty relations for the support of quantum states

Vincenzo Fiorentino[*] and **Stefan Weigert**[*]

Department of Mathematics, University of York, York YO10 5DD, United Kingdom

E-mail: vincenzo.fiorentino@york.ac.uk and stefan.weigert@york.ac.uk

Abstract

Given a narrow signal over the real line, there is a limit to the localisation of its Fourier transform. In spaces of prime dimensions, Tao derived a sharp state-independent uncertainty relation which holds for the support sizes of a pure qudit state in two bases related by a discrete Fourier transform. We generalise Tao's uncertainty relation to complete sets of mutually unbiased (MU) bases in spaces of prime dimensions. The bound we obtain appears to be sharp for dimension three only. Analytic and numerical results for prime dimensions up to nineteen suggest that the bound cannot be saturated in general. For prime dimensions two to seven we construct sharp bounds on the support sizes in $(d+1)$ MU bases and identify some of the states achieving them.

Keywords: uncertainty relations, support size, support inequality, mutually unbiased bases, prime dimensions, support uncertainty relation

1. Introduction

No quantum particle can reside in a state with both its position and momentum distributions being localised arbitrarily well. For these incompatible observables, Heisenberg's uncertainty relation [1, 2] establishes a finite lower bound for the product of their variances. This result relies on a fundamental property of Fourier theory: a real (or complex) function with *finite* support on the real line has a Fourier transform which must be non-zero almost everywhere [3]. It is, however, difficult to quantify the support of functions on unbounded intervals. Using variances instead of the supports of probability distributions circumvents this difficulty.

---

[*] Authors to whom any correspondence should be addressed.

The situation is different for quantum systems with finite-dimensional Hilbert spaces since the *support (size)* of a pure state—defined as the number of non-zero components in a given orthonormal basis—is always finite. A computational basis state in $\mathbb{C}^d$, say, has support equal to one, and the support of its (discrete) Fourier transform equals d since all basis states contribute. Thus, the *product* of the support sizes equals d which turns out to be its smallest possible value [4].

The underlying product inequality has been generalised in a number of directions [5, 6]. Tao derived an *additive* inequality [7] which is valid in spaces $\mathbb{C}^d$ of prime dimensions $d = p$: the *sum* of the supports of a state and its discrete Fourier transform is bounded from below by the value $(p + 1)$. This bound is sharp since a computational basis state and its Fourier transform saturate it.

Support inequalities and their generalisations have found applications in signal processing [8, 9], for example, and they can be used to identify non-classical quantum states [10] whose Kirkwood–Dirac quasiprobability distribution [11, 12] is *not* a probability distribution. Such states provide an advantage in quantum metrology [13] and play a role in weak measurements [14–16] and contextuality [17].

Using the support size of a quantum state as a measure of uncertainty has an unexpected—and previously unnoticed—operational advantage. Quantum supports take a *finite* set of integer values only, in stark contrast to other measures. Variances of observables in a given state or its von Neumann entropy take *real numbers* as values which demands many measurements to determine experimentally. However, a *finite* number of measurements may already suffice to determine the *exact* support size of a quantum state. This situation occurs whenever the state at hand has (a) 'full' support in the basis considered and (b) each outcome has been registered at least once. Conformity with a given support inequality may be verified by a *finite* number of measurements as small as the bound itself. This property depends, of course, on the assumption that outcomes with probability zero never occur; limited detection efficiency does not invalidate the argument, however.

Variance-based uncertainty relations also exist for more than two observables associated with multiple orthonormal bases [18–21]: position and momentum may be supplemented by a third continuous variable which is canonical to each of them. The eigenbases of these three observables are mutually unbiased (MU) and related by fractional Fourier transforms. The product of their variances satisfies a *triple uncertainty relation* [18]. Importantly, the lower bound of this inequality does *not* follow from the pair uncertainty relations but must be determined independently. No quantum state exists which satisfies all three pair uncertainty relations simultaneously. In a similar vein, entropic uncertainty relations capture the incompatibility of up to $(d + 1)$ observables in finite-dimensional systems, linked to a complete set of MU bases known to exist in prime-power dimension [22–24].

The main goal of this paper is to extend Tao's additive support uncertainty relation to the case of more than two bases, inspired by the triple uncertainty relation for continuous variables. The focus will be on prime-dimensional spaces where $(p + 1)$ MU bases exist, known as *complete sets*. The support sizes of a state in any pair of MU bases from such a set are expected to satisfy Tao's bound but it is unlikely that they will saturate all pair bounds simultaneously.

This paper is structured as follows. Section 2 sets up notation by briefly describing known product and sum inequalities for the support of a vector, and the properties of complete sets of MU bases are summarised. In section 3, Tao's additive uncertainty relation for the support of quantum states is shown to hold for any pair of MU bases in the complete set considered, and the generalised additive support inequality involving all $(p + 1)$ MU bases is established as a direct consequence. According to section 4 the bounds provided by the generalised support

inequality cannot be saturated for prime dimensions $2 \leqslant d \leqslant 19$, except $d = 3$. Higher *achievable* bounds are derived in section 5, for prime numbers up to $d = 7$. In the last section, we summarise and discuss the results obtained. The proofs of some lemmata are relegated to an appendix.

2. Preliminaries

2.1. Support inequalities for a Fourier pair of bases

The *support* (*size*) of a Hilbert-space vector $\psi \in \mathcal{H}_d$ is given by the number of its non-zero expansion coefficients $\psi_v = \langle v | \psi \rangle$ in an orthonormal basis $\mathcal{B} = \{|v\rangle, v = 0, 1, \ldots, d-1\}$,

$$|\text{supp}(\psi, \mathcal{B})| = \#(\psi_v \neq 0, v = 0 \ldots d-1) \in \{0 \ldots d\}. \tag{1}$$

The only vector with vanishing support is the zero vector. Due to normalisation, the support of a quantum state must be at least one, and the maximum is achieved whenever the state ψ is a linear combination of all d basis states. The support size of a state clearly depends on the chosen basis. Formally, the support size can be obtained as a limit of the Rényi entropy [25] of the probability distribution $\{|\psi_v|^2, v = 0 \ldots d-1\}$.

Thinking of the support size as the (improper) L^0-'norm' of ψ, we will use the notation

$$|\text{supp}(\psi, \mathcal{B})| = \|\psi\|_{\mathcal{B}}. \tag{2}$$

The set of expansion coefficients $\{\psi_v, v = 0 \ldots d-1\}$ has three obvious *support-conserving* symmetries. The support size is invariant (a) under rephasing each expansion coefficient separately,

$$\|\psi\|_{\mathcal{B}} = \|R\psi\|_{\mathcal{B}}, \qquad R = \text{diag}(e^{i\tau_0}, e^{i\tau_1}, \ldots, e^{i\tau_{d-1}}), \tag{3}$$

with real numbers $\tau_v, v = 0, \ldots, d-1$; (b) under permuting the components of any state among themselves

$$\|\psi\|_{\mathcal{B}} = \|P\psi\|_{\mathcal{B}}, \qquad P \in S_d, \tag{4}$$

where S_d is the permutation group acting on sets of d elements; and (c) under the complex conjugation of some (or all) of its components,

$$\|\psi\|_{\mathcal{B}} = \|K\psi\|_{\mathcal{B}}, \qquad K = \prod_{\text{some } v \in \{0 \ldots d-1\}} K_v, \tag{5}$$

where each operator $K_v, v = 0, \ldots, d-1$, maps one expansion coefficient of the state ψ in the basis $\mathcal{B}$ to its complex conjugate, $K_v \psi_v = \psi_v^*$, and does not change the others. In the basis $\mathcal{B}$, the permutations P are represented by a matrix of order d containing exactly one unit entry in each row and column; hence the unitary invariances of rephasing and permuting coefficients are conveniently combined into *monomial* matrices $M \equiv RP$. The third invariance described by the operators K_v will play no role.

Given two distinct orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of $\mathcal{H}_d$, one may ask to which extent a state can be 'localised' in both of them. Clearly, the product of its support sizes in $\mathcal{B}$ and $\mathcal{B}'$ may take values between one and d^2. If the bases are related by $\mathcal{B}' = F\mathcal{B}$, where F is the discrete Fourier transform with matrix elements (in the $\mathcal{B}$-basis)

$$F_{vv'} = \frac{1}{\sqrt{d}} e^{-2\pi i v v'/d} \qquad v, v' \in \{0 \ldots d-1\}, \tag{6}$$

then the *product* of the support sizes of a state ψ and its Fourier transform $\widetilde{\psi} = F^\dagger \psi$ is bounded from below [4],

$$\|\psi\|_{\mathcal{B}} \|\psi\|_{\mathcal{B}'} \geqslant d, \tag{7}$$

where we use the fact that the support size of the Fourier transformed state $\widetilde{\psi}$ in the basis $\mathcal{B}$ is equal to the support size of the state ψ in the basis $\mathcal{B}'$, i.e.

$$\|\widetilde{\psi}\|_{\mathcal{B}} = \|F^\dagger \psi\|_{\mathcal{B}} = \|\psi\|_{\mathcal{B}'}. \tag{8}$$

The inequality (7) represents a finite-dimensional equivalent of Heisenberg's uncertainty relation for position and momentum observables of a quantum particle: quantum states localised in position, say, necessarily come with a broad variance in momentum, the Fourier-transformed position observable.

For spaces $\mathcal{H}_d$ with *prime* dimensions d, an *additive* inequality for the supports of a quantum state in a pair of Fourier-related bases is known [7],

$$\|\psi\|_{\mathcal{B}} + \|\psi\|_{\mathcal{B}'} \geqslant d+1, \tag{9}$$

which is stronger than the multiplicative relation (7), as follows from the inequality $d+1-x \geqslant d/x$, for $x \in [1,d]$. In the terminology of [10], any two bases $\mathcal{B}$ and $\mathcal{B}'$ are said to be *completely incompatible* if and only if the support sizes of the expansion coefficients of any (non-zero) vector $\psi \in \mathcal{H}_d$ satisfy this bound.

The inequality (9) is a special case of a theorem valid for finite additive Abelian groups G with $|G|$ elements and trivial subgroups only which necessitates the restriction to prime dimensions [7]. Consider a complex-valued function $f : G \to \mathbb{C}$ and its transform $\widetilde{f} : G \to \mathbb{C}$, defined by

$$\widetilde{f}(v') = \frac{1}{\sqrt{|G|}} \sum_{v \in G} f(v) \overline{e(v,v')}, \tag{10}$$

where $e(v,v')$ is a 'bi-character' of G satisfying $e(v_1 + v_2, v') = e(v_1, v') e(v_2, v')$ and an analogous relation for its second argument. In the particular case of $e(v,v') = e^{-2\pi i v v'/d}$, one obtains an inequality for the supports of f and $\widetilde{f} \equiv F^\dagger f$.

Theorem 1 (Tao's theorem). *If $f : G \to \mathbb{C}$ is a non-zero function and the cardinality $|G|$ of the group G is prime, then*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\widetilde{f})| \geqslant |G|+1. \tag{11}$$

Upon identifying $f(v)$ with $\langle v|\psi \rangle$ and $\widetilde{f}(v')$ with $\langle v'|\psi \rangle$, respectively, we obtain the inequality (9) relative to the bases $\mathcal{B}$ and $\mathcal{B}'$ introduced via F in equation (6).

The main ingredient of Tao's proof is a fundamental property of the Fourier matrix in prime dimensions [7, 26, 27] which dates back to the 1920s: all its square submatrices are invertible.

Theorem 2 (Chebotarëv's theorem). *If d is prime, then all minors of the Fourier matrix F in equation (6) are non-zero.*

The inequalities (7) and (9) involve a *pair* of MU bases of $\mathcal{H}_d$, namely the computational basis $\mathcal{B}$ and its Fourier transform. We will now introduce larger sets of MU bases to formulate more general support inequalities. Not surprisingly, Chebotarëv's theorem must be generalised to other matrices which emerge when establishing bounds on support sizes of quantum states in multiple bases (cf section 3.1).

2.2. MU bases in prime dimensions

Two orthonormal bases of the space $\mathcal{H}_d = \mathbb{C}^d$ are said to be MU if the inner products between any two states (not of the same basis) have modulus $1/\sqrt{d}$. Then, to know the outcome of a projective measurement performed in one basis implies complete uncertainty about the outcome of a subsequent projective measurement performed in the other.

When d is a power of a prime number p, i.e. $d = p^n$, sets of $(d+1)$ MU bases have been constructed [28–31]. Such complete sets are both *maximal*—in the sense that no additional MU basis can be added to it—and *tomographically complete*: the probability distributions of outcomes in the $(d+1)$ bases uniquely encode an unknown quantum state. It is an open problem whether complete sets of MU bases exist in composite dimensions, $d \neq p^n$.

For $d = 2$, the eigenstates of the Pauli operators Z_2, X_2 and $X_2 Z_2 = -iY_2$ form a complete set which has a simple structure. Representing the computational basis $\mathcal{B}_0$ by the identity matrix $H_0 = I_{(2 \times 2)}$, the following two Hadamard matrices encode the bases which are MU to $\mathcal{B}_0$,

$$H_1 = F = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad H_2 = DF \quad \text{where } D = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \qquad (12)$$

If d is an odd prime, the eigenstates of the $(d+1)$ generalised Pauli operators Z_d, X_d, $X_d Z_d$, $X_d Z_d^2$, ..., $X_d Z_d^{d-1}$, represent a maximal set of MU bases. The kth state of the jth basis is given by

$$|\phi_k^j\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} \omega^{-kx} \omega^{(j-1)x^2} |\phi_x^0\rangle, \qquad j \in \{1 \dots d\}, \quad k \in \{0 \dots d-1\}, \qquad (13)$$

where the states $\{|\phi_x^0\rangle \equiv |x\rangle, x = 0 \dots d-1\}$ form the computational basis $\mathcal{B}_0$ and $\omega \equiv e^{2i\pi/d}$ is a dth root of the number 1 [31]. For each value of j, the equimodular expansion coefficients

$$[H_j]_{xk} = \langle x|\phi_k^j\rangle = \frac{1}{\sqrt{d}} \omega^{-kx} \omega^{(j-1)x^2}, \qquad j \in \{1 \dots d\}, x, k \in \{0 \dots d-1\}, \qquad (14)$$

define a *complex-valued Hadamard matrix*. These are unitary matrices since their columns are given by the components (in the computational basis $\mathcal{B}_0$) of d orthogonal vectors. When combined with the computational basis $\mathcal{B}_0$, the states given in equation (13) form a complete set of MU bases for Hilbert spaces of prime dimensions, which we will refer to as the *standard* set. In this paper, all MU bases will be taken from the standard set.

The Hadamard matrix H_1 in (14) coincides with the discrete Fourier matrix F given in equation (6). The remaining Hadamard matrices H_j map the computational basis $\mathcal{B}_0$ of $\mathcal{H}_d$ to other orthonormal bases denoted by $\mathcal{B}_j$. Adopting an active view of these transformations, the state ψ is mapped to the state $H_j^\dagger \psi$. The relation between the supports of the state ψ in $\mathcal{B}_0$ and the jth MU basis $\mathcal{B}_j$ reads,

$$\|H_j^\dagger \psi\|_0 = \|\psi\|_j, \qquad (15)$$

abbreviating the notation introduced in (8), i.e. $\|\psi\|_{\mathcal{B}_j} \equiv \|\psi\|_j$, $j \in \{0 \dots d\}$.

The columns of the d Hadamard matrices H_j in (14) are related in a simple way to each other, namely by

$$|\phi_k^j\rangle = D^{j-1} B^k |\phi_0^1\rangle, \qquad j \in \{1 \dots d\}, k \in \{0 \dots d-1\}, \qquad (16)$$

with two diagonal $(d \times d)$ matrices B and D; in other words, all states of the complete set of MU bases can be generated easily from any given state such as $|\phi_0^1\rangle$—except for the states

of the computational basis $\mathcal{B}_0$. Within each Hadamard matrix, the matrix B cyclically shifts a given column to the right,

$$B|\phi_k^j\rangle = \begin{cases} |\phi_{k+1}^j\rangle, & k = 0,\ldots,d-2, \\ |\phi_0^j\rangle, & k = d-1; \end{cases} \tag{17}$$

its entries are given by the components of the second column of the Fourier matrix $F = H_1$,

$$B = \operatorname{diag}\left(1, \omega^{-1}, \ldots, \omega^{-(d-1)}\right), \tag{18}$$

except for the factor $\sqrt{d}$.

The matrix D is given by the components of the first column of the second Hadamard matrix H_2, i.e.

$$D = \operatorname{diag}\left(1, \omega^1, \ldots, \omega^{(d-1)^2}\right), \tag{19}$$

cyclically mapping a state of the jth MU basis to the corresponding one of the MU basis with label $(j+1)$,

$$D|\phi_k^j\rangle = \begin{cases} |\phi_k^{j+1}\rangle, & j = 1,\ldots,d-1, \\ |\phi_k^1\rangle, & j = d. \end{cases} \tag{20}$$

In terms of Hadamard matrices, this property reads

$$DH_j = \begin{cases} H_{j+1}, & j = 1,\ldots,d-1, \\ H_1, & j = d. \end{cases} \tag{21}$$

Writing $H_j = D^{j-1}H_1 \equiv D^{j-1}F$, Chebotarëv's theorem is seen to imply that the minors of all Hadamard matrices H_j, $j = 1\ldots d$, are non-zero: the ranks of the minors of F do not change upon multiplying their rows with non-zero scalars. In view of equation (12), this generalisation is also valid for the case of $d = 2$.

3. Support inequalities...

How well can one localise quantum states simultaneously in $(d+1)$ MU bases? To answer this question, we need to minimise the support sizes of a state relative to the complete set. In a first step, we now show that the support sizes of a quantum state relative to any *pair* of standard MU bases also satisfy Tao's bound (9). Second, by combining the resulting pair inequalities, we establish a state-independent lower bound.

3.1. ... for arbitrary pairs of MU bases

Tao's result establishes—for a space of prime dimension d supporting a cyclic abelian group— a sharp inequality for the support sizes of a quantum state and its Fourier transform. Most pairs of the MU bases introduced in equation (13) are, however, not related by a Fourier transform. Nevertheless, Tao's bound also holds for the supports of the images of any quantum state generated by two Hadamard matrices as we will show now.

Theorem 3. *Given any pair of distinct standard MU bases associated with matrices H_j and H_k, $j, k \in \{0\ldots d\}$, the support sizes of a quantum state $|\psi\rangle \in \mathcal{H}_d$ satisfy the state-independent sharp bound,*

$$\|\psi\|_j + \|\psi\|_k \geqslant d+1, \tag{22}$$

where d is any prime number.

It is important to realise that theorem 3 does not cover *arbitrary* pairs of MU bases in prime dimensions but only those defined in equation (14). Nevertheless, *all* pairs of MU bases in dimensions $d = 2, 3$ and 5 are found to be completely incompatible since in these dimensions *all* Hadamard matrices are equivalent to the Fourier matrix. Already for the next prime, $d = 7$, other types of Hadamard matrices exist [32].

Proof. The case of dimension $d = 2$ is straightforward. If a state $|\psi\rangle \in \mathcal{H}_2$ has support one in one MU basis, it must have support two in both other bases, due to being MU to their members. Thus, the sum of the supports of any state in two bases must be at least three.

For odd primes d, we will consider two cases separately: either (a) one of the bases in equation (22) is the computational basis, so that $j = 0$, say, or (b) neither of them.

(a) Defining the vector $\phi = D^{1-k}\psi$, we obtain

$$\|\psi\|_0 + \|\psi\|_k = \|\psi\|_0 + \|H_k^\dagger \psi\|_0 = \|\psi\|_0 + \|F^\dagger D^{1-k}\psi\|_0$$
$$= \|D^{k-1}\phi\|_0 + \|F^\dagger \phi\|_0, \tag{23}$$

recalling that $H_k = D^{k-1}F$ holds according to equation (21). Since D is a diagonal unitary hence a support-conserving unitary matrix (cf (3)), we obtain

$$\|\psi\|_0 + \|\psi\|_k = \|\phi\|_0 + \|F^\dagger \phi\|_0 \geqslant d + 1, \tag{24}$$

where Tao's theorem was used in the last step.

(b) Now consider the case where the non-zero labels j and k differ from each other. Defining the vector $\phi = H_j^\dagger \psi$, the sum of the support sizes can be written as

$$\|\psi\|_j + \|\psi\|_k = \|H_j^\dagger \psi\|_0 + \|H_k^\dagger \psi\|_0 = \|\phi\|_0 + \|H_k^\dagger H_j \phi\|_0. \tag{25}$$

The product $H_k^\dagger H_j$ of two distinct Hadamard matrices is, in fact, always equal to another Hadamard matrix $H_t^\dagger$, $t \neq 0$, up to a monomial matrix $M(j,k)$; this result is the content of lemma 1 stated directly after the proof. As the matrix $M(j,k)$ is support-conserving (cf equations (3) and (4)) for all states of the space $\mathcal{H}_d$, we find

$$\|\phi\|_0 + \|M(j,k)H_t^\dagger \phi\|_0 = \|\phi\|_0 + \|H_t^\dagger \phi\|_0 \geqslant d + 1, \tag{26}$$

where (24) of part (a) has been used in the final step. $\qquad\square$

The proof just relies on dissolving products of the Hadamard matrices H_j which encode a complete set of MU bases. Clearly, products of the form $H_k^\dagger H_j$, $j \neq k$, are Hadamard matrices since their matrix elements, being overlaps of MU vectors, have modulus $1/\sqrt{d}$,

$$\left[H_k^\dagger H_j\right]_{\ell\ell'} = \langle \phi_\ell^k | \phi_{\ell'}^j \rangle. \tag{27}$$

When $d = 2$, one finds explicitly that $H_1^\dagger H_2 = MH_2^\dagger$ and $H_2^\dagger H_1 = M'H_2^\dagger$, with monomial matrices M and M'. In other words, the phases of the matrix elements (27) coincide with those of the adjoint of another transition matrix after permuting and rephasing its rows. This property actually holds for any prime dimension.

Lemma 1. *Let d be an odd prime and $j, k \in \{1 \ldots d\}$ with $j \neq k$. Then*

$$H_k^\dagger H_j = M(j,k)H_t^\dagger \tag{28}$$

for a monomial matrix $M(j,k)$ if and only if $t = 1 + \chi \in \{1, \ldots, d\}$ where the integer χ satisfies $4(j-k)\chi = 1 \mod d$.

Proof. See appendix. $\qquad\square$

Furthermore, lemma 1 allows us to generalise Chebotarëv's theorem to the product matrices $H_k^\dagger H_j$, for distinct indices j and k.

Corollary 1. *If d is prime, then all minors of the Hadamard matrices $H_k^\dagger H_j$, $j,k \in \{0\dots d\}$ and $j \neq k$, are non-zero.*

Proof. Let d be an odd prime. Any H_t, $t \in \{1\dots d\}$, has only non-zero minors, as was mentioned after equation (21), as do the adjoints $H_t^\dagger$. Therefore, the claim holds if one of the labels j,k, is zero. For both $j,k \neq 0$, lemma 1 applies. Since rephasing and permuting the rows of a matrix do not change the rank of any submatrix, we can conclude that the matrices $H_k^\dagger H_j$, $j,k \neq 0$ and $j \neq k$ also have non-zero minors only.

In dimension $d = 2$, the result follows from inspecting the products $H_1^\dagger H_2 = M H_2^\dagger$ and $H_2^\dagger H_1 = M' H_2^\dagger$. $\qquad\square$

According to corollary 1 the vectors formed by the columns (or rows) of all square submatrices of the Hadamard matrices $H_k^\dagger H_j$, $j \neq k$, are linearly independent. What is more, up to d vectors taken from *any two* MU bases are linearly independent.

Corollary 2. *Given a complete standard set of MU bases in the space $\mathcal{H}_d$ of prime dimension d, up to d vectors taken from any two MU bases are linearly independent.*

Proof. See appendix. $\qquad\square$

Theorem 3 also demonstrates that all pairs of MU bases taken from the complete standard set in prime dimension are *completely incompatible*, in the sense of section 2.1. This statement is stronger than the results of [7, 10] since the bases we consider are not necessarily related by the Fourier matrix F.

3.2. … for complete sets of $(d+1)$ MU bases

Let us denote the sum of the numbers of non-zero expansion coefficients of a state $\psi \in \mathcal{H}_d$ in a complete standard set of MU bases by

$$\mathcal{S}(d) = \|\psi\|_0 + \|\psi\|_1 + \cdots + \|\psi\|_d. \tag{29}$$

Then, the inequalities (22) imply that the overall support size $\mathcal{S}(d)$ cannot fall below a certain threshold. This is a central result of our paper.

Theorem 4. *For any prime d, the overall support $\mathcal{S}(d)$ of a quantum state $|\psi\rangle \in \mathcal{H}_d$ in a complete standard set of MU bases satisfies the additive state-independent bound*

$$\mathcal{S}(d) \geqslant \frac{(d+1)^2}{2} \equiv T(d). \tag{30}$$

Proof. Write down $(d+1)$ copies of the support inequality (22) with indices $(j, j+1)$, $j = 0, \dots d-1$, and $(d,0)$, respectively. Adding them up, the right-hand-sides of (22) give $(d+1)^2$, and since each term $\|\psi\|_j \equiv \|H_j^\dagger \psi\|_0$, $j = 0, \dots, d$, occurs twice on the left, one obtains the inequality (30). $\qquad\square$

An alternative proof treats all pair supports equally: write down (22) for all $d(d+1)$ distinct pairs of indices (j,k) and consider the sum of the supports. After removing common factors, the bound (30) on $\mathcal{S}(d)$ follows.

Support inequalities other than equations (22) and (30) exist. They may involve any number between two and $(d+1)$ MU bases. For example, picking the first three MU bases and combining the associated pair inequalities from (22) leads to the additive 'triple support inequality',

$$\mathcal{S}(d;3) \equiv \|\psi\|_0 + \|F^\dagger \psi\|_0 + \|H_2^\dagger \psi\|_0 \geqslant \frac{3}{2}(d+1). \tag{31}$$

Clearly, this inequality cannot be saturated for dimension $d = 2$ because the overall support $\mathcal{S}(2)$ of a state is always an integer number. Taking only two possible values, the smallest achievable value of the triple support size $\mathcal{S}(2;3) \equiv \mathcal{S}(2)$ equals $T_s(2) = 5$; here and in the following, *achievable*—or *sharp*—bounds of $\mathcal{S}(d)$ are denoted by $T_s(d)$.

The lower bound on the triple uncertainty relation for continuous variables [18], derived similarly by combining pair uncertainty relations, can also not be reached. Theorem 4 is not constructive, hence it is not obvious whether the case of $d = 2$ represents an exception or whether the inequalities (30) are never sharp. In the next section we will first derive some general results about multiple-support inequalities, followed by a closer look at dimensions $3 \leqslant d \leqslant 19$.

4. Saturating support inequalities for MU bases

To saturate the bound of the inequality (30) means to identify states that minimise all support pair relations simultaneously. We present a number of rigorous results for prime dimensions $d \leqslant 7$. Numerical methods are then used to determine whether the generalised inequality can be saturated for dimensions up to $d = 19$.

4.1. Constraints on saturating states

Our first general result is a necessary and sufficient condition that the support inequality (30) involving a complete set of $(d+1)$ MU bases be saturated.

Theorem 5 (Equal support sizes). *The additive support inequality for a complete standard set of MU bases (30) is saturated by a state $\psi \in \mathcal{H}_d$ if and only if it has the same support in all $(d+1)$ MU bases, i.e.*

$$\|\psi\|_j = \frac{d+1}{2}, \qquad j \in \{0 \dots d\}, \tag{32}$$

where d is an odd prime.

Proof. Substituting the values (32) into (30) directly produces the lower bound.

For the converse, we show that the supports must have the values given in (32) if equality holds in equation (30). Noting that the support of any state $\psi \in \mathcal{H}_d$ ranges from 1 to d, i.e.

$$\|\psi\|_0 = \frac{d+1}{2} \pm \Delta, \qquad \Delta \in \left\{0, 1, \dots, \frac{1}{2}(d-1)\right\}, \tag{33}$$

we will proceed by exhausting all its values in the computational basis $\mathcal{B}_0$. It turns out that the minimum in (30) cannot be reached if the support is either (a) smaller or (b) larger than $(d+1)/2$, leaving (c) the values in (32) as the only option.

(a) If $\|\psi\|_0 = (d+1)/2 - \Delta$, $\Delta > 0$, then (22) implies that $\|\psi\|_j \geqslant (d+1)/2 + \Delta$, $j = \{1 \ldots d\}$. Hence, the sum of the supports in all $(d+1)$ MU bases equals

$$\mathcal{S}(d) = \sum_{j=0}^{d} \|\psi\|_j \geqslant \frac{d+1}{2} - \Delta + d \left(\frac{d+1}{2} + \Delta \right)$$
$$\geqslant \frac{(d+1)^2}{2} + (d-1)\Delta > \frac{(d+1)^2}{2}. \tag{34}$$

Therefore, the inequality cannot be saturated by a state which has support smaller than $(d+1)/2$ in the basis $\mathcal{B}_0$.

(b) Assume that $\|\psi\|_0 = (d+1)/2 + \Delta$, $\Delta > 0$. Clearly, the lower bound of the sum in equation (30) can only be reached if the support of the state ψ is smaller than $(d+1)/2$ in at least one of the MU bases, $\|\psi\|_{j^*} < (d+1)/2$, $j^* \in \{1 \ldots d\}$, say. Repeating the argument from (a) relative to the MU basis $\mathcal{B}_{j^*}$ instead of $\mathcal{B}_0$ implies that the inequality (30) cannot be saturated.

(c) If $\|\psi\|_0 = (d+1)/2$ then (22) implies that $\|\psi\|_j \geqslant (d+1)/2$, $j = \{1 \ldots d\}$. However, given these bounds, the minimum of $\mathcal{S}(d)$ in (30) can be achieved only if the support of the state $\psi \in \mathcal{H}_d$ takes the value $(d+1)/2$ in all other MU bases as well. $\qquad \square$

The second general result states that a specific dth root of unity can appear at most *twice* in the columns of the Hadamard matrices H_j, $j = 2 \ldots d$, given in (14). The proof of another necessary–but not sufficient–condition for saturating the generalised inequality (30) will rely on this limit of the occurrences of roots. The property also applies to to $H_1 \equiv F$ where each root appears exactly once in every column, as is seen by inspecting (6).

Lemma 2 (Frequency of roots). *Let d be prime and consider the states $|\phi_k^j\rangle$, $j = 2, \ldots, d$, in equation (13) forming the bases $\mathcal{B}_j$ which are MU to both the identity and the Fourier matrix. Any dth root ω^n, $n \in \{0 \ldots d\}$, figures at most twice among the numbers $\sqrt{d}\langle x|\phi_k^j\rangle$, $x \in \{0 \ldots d-1\}$.*

Proof. We need to determine the number of solutions of the equation $\omega^{-kx+(j-1)x^2} = \omega^n$ which becomes $(j-1)x^2 - kx - n \mod d = 0$ upon taking the logarithm and rearranging. Since $j \neq 1$, the equation is quadratic for each n and there can be at most two integer solutions for the unknown x. The extension to the special case of $d = 2$ is trivial. $\qquad \square$

According to theorem 5, a state saturating (30) must have $(d-1)/2$ vanishing expansion coefficients in each MU basis of the standard set, in any odd prime dimension. A third general result is that there are constraints on the distributions of these zeroes when expanded in the MU bases of a complete set.

To spell out these constraints, let us introduce the *zero distributions* $\mathcal{Z}^j$ of a state $\psi \in \mathcal{H}_d$ which list the indices of the vanishing expansion coefficients in the $(d+1)$ bases of the complete set,

$$\mathcal{Z}^j = \left\{ \kappa \in \{0 \ldots d-1\} : \langle \phi_\kappa^j | \psi \rangle = 0 \right\}, \qquad j = 0, \ldots, d. \tag{35}$$

Using the relation $\langle \phi_\kappa^j | \psi \rangle = \langle \phi_\kappa^0 | H_j^\dagger | \psi \rangle$, one can also think of $\mathcal{Z}^j$ as the set of vanishing coefficients of the state $H_j^\dagger | \psi \rangle$ in the computational basis.

Two zero distributions of vectors in the same Hilbert space are said to be *compatible*, $\mathcal{Z} \sim \mathcal{Z}'$, if they are equal up to a cyclic shift. In other words, two compatible distributions $\mathcal{Z} = \{\kappa_1, \kappa_2, \ldots, \kappa_\delta\}$ and $\mathcal{Z}' = \{\kappa_1', \kappa_2', \ldots, \kappa_\delta'\}$ must have the same number δ of elements and the mapping $\kappa_i \mapsto \kappa_i + \mu \mod d$ for some fixed integer μ must be a bijection from $\mathcal{Z}$ to $\mathcal{Z}'$. Compatibility of zero distributions is an equivalence relation between classes of d elements.

The extension of Chebotarëv's theorem shown in section 3.1 and lemma 2 imply a constraint on zero distributions for all prime dimensions $d > 3$. This property will be used in section 4.3 to prove that the support inequality (30) *cannot* be saturated in dimensions $d = 5$ and $d = 7$.

Theorem 6. *Let $d > 3$ be prime and $\psi \in \mathcal{H}_d$ be a state with $(d-1)/2$ expansion coefficients vanishing in the computational basis and in two more standard MU bases, i.e.*

$$\|\psi\|_0 = \|\psi\|_{j_1} = \|\psi\|_{j_2} = \frac{d+1}{2}, \qquad j_1 > j_2 \neq 0. \tag{36}$$

Then the zero distributions associated with the vectors $H_{j_1}^\dagger |\psi\rangle$ and $H_{j_2}^\dagger |\psi\rangle$, respectively, are incompatible.

Proof. Since the state ψ has $d_- \equiv (d-1)/2$ vanishing components in three bases with labels $j = 0, j_1, j_2$, it satisfies $3d_-$ conditions,

$$\begin{aligned}
\langle \phi_{\kappa_1^0}^0 |\psi\rangle = \langle \phi_{\kappa_2^0}^0 |\psi\rangle = \ldots = 0, \qquad & \mathcal{Z}^0 = \left\{ \kappa_1^0, \kappa_2^0, \ldots, \kappa_{d_-}^0 \right\}, \\
\langle \phi_{\kappa_1^1}^{j_1} |\psi\rangle = \langle \phi_{\kappa_2^1}^{j_1} |\psi\rangle = \ldots = 0, \qquad & \mathcal{Z}^{j_1} = \left\{ \kappa_1^1, \kappa_2^1, \ldots, \kappa_{d_-}^1 \right\}, \\
\langle \phi_{\kappa_1^2}^{j_2} |\psi\rangle = \langle \phi_{\kappa_2^2}^{j_2} |\psi\rangle = \ldots = 0, \qquad & \mathcal{Z}^{j_2} = \left\{ \kappa_1^2, \kappa_2^2, \ldots, \kappa_{d_-}^2 \right\}.
\end{aligned} \tag{37}$$

We proceed by contradiction. To assume that the zero distributions $\mathcal{Z}^{j_1}$ and $\mathcal{Z}^{j_2}$ *are* compatible means that they are related by a cyclic shift by some integer $\mu \in \{0 \ldots d-1\}$. In particular, we can arrange the elements in the two sets such that

$$\kappa_i^2 = \kappa_i^1 + \mu \mod d \qquad \text{for all} \quad i \in \{1 \ldots d_-\}. \tag{38}$$

Then, according to equation (16), the corresponding states must be related by powers of the matrices D and B,

$$|\phi_{\kappa_i^2}^{j_2}\rangle = D^{j_2-1} B^{\kappa_i^2} |\phi_0^1\rangle = D^{j_2-1} B^{\kappa_i^2} D^{-j_1+1} B^{-\kappa_i^1} |\phi_{\kappa_i^1}^{j_1}\rangle = D^{j_2-j_1} B^\mu |\phi_{\kappa_i^1}^{j_1}\rangle, \tag{39}$$

where we have used the fact that D and B commute. Defining $V_\mu^\dagger = D^{j_2-j_1} B^\mu$, the third set of conditions in (37) turns into

$$\langle \phi_{\kappa_i^2}^{j_2} |\psi\rangle = \langle \phi_{\kappa_i^1}^{j_1} | V_\mu \psi\rangle = 0 \qquad \text{for all} \quad i \in \{1 \ldots d_-\}. \tag{40}$$

Since V_μ is diagonal in the computational basis, we have

$$\langle \phi_{\kappa_i^0}^0 |\psi\rangle = \langle \phi_{\kappa_i^0}^0 | V_\mu \psi\rangle = 0 \qquad \text{for all} \quad i \in \{1 \ldots d_-\}, \tag{41}$$

which means that $\mathcal{Z}^0$ and $\mathcal{Z}^{j_1}$ are zero distributions for the pair of vectors ψ and $V_\mu \psi$. In other words, these two states are both orthogonal to the same set of $2d_- = (d-1)$ vectors

$$\left\{ \phi_{\kappa_1^0}^0, \ldots, \phi_{\kappa_{d_-}^0}^0, \phi_{\kappa_1^1}^{j_1}, \ldots, \phi_{\kappa_{d_-}^1}^{j_1} \right\}, \tag{42}$$

stemming from the computational basis $\mathcal{B}_0$ and the basis $\mathcal{B}_{j_1}$. According to corollary 2, this is a set of $(d-1)$ linearly independent vectors so that only one unique ray in $\mathcal{H}_d$ can exist that is orthogonal to all of them. Therefore, the vectors ψ and $V_\mu \psi$ must be collinear, i.e. $V_\mu \psi = \lambda \psi$ for some non-zero scalar $\lambda \in \mathbb{C}$.

Since $V_\mu = D^{j_1-j_2} B^{-\mu}$ is diagonal in $\mathcal{B}_0$, the computational basis states are eigenvectors of V_μ. By assumption, the state ψ has $d_+ \equiv (d+1)/2$ non-zero coefficients in this basis. Thus, the state ψ will be an eigenvector of the unitary V_μ only if λ is an eigenvalue with multiplicity of d_+ (at least). However, this is impossible for prime dimensions $d > 3$: the non-zero matrix

elements on the diagonal of V_μ coincide with the components of the vector $\sqrt{d}|\phi_{-\mu}^{j_1-j_2+1}\rangle$ in the computational basis but for $j_1 > j_2 \neq 0 \,(\mathrm{mod}\,d)$ no more than two of the components may coincide according to lemma 2. Thus, at most two of the eigenvalues of V_μ can coincide. No contradiction arises for dimension $d = 3$ where ψ has exactly two non-vanishing coefficients in the computational basis. $\qquad\square$

4.2. Dimension $d = 3$

To prove that the bound (30) can be achieved in the space $\mathcal{H}_3$, we exhibit the states which minimise the support inequality.

Theorem 7. *The state ψ saturates the generalised support inequality (30) in dimension $d = 3$ if and only if it is one of the following nine (non-normalised) qutrit states,*

$$\begin{pmatrix} 1 \\ -\omega^m \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ -\omega^m \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ -\omega^m \end{pmatrix}, \qquad m \in \{0, 1, 2\}, \tag{43}$$

with $\omega \equiv e^{2i\pi/3}$ being a third root of unity.

Proof. Theorem 5 implies that a state ψ saturates equation (30) w.r.t. a complete standard set of MU bases if and only if it has support two in each of them, i.e. $\|\psi\|_j \equiv \|H_j^\dagger \psi\|_0 = 2$, $j = 0 \ldots 3$. First, we assume that the third component of a candidate state vanishes in the computational basis, i.e. $\psi = (a, b, 0)^T$, with non-zero complex numbers a and b. Applying the matrices $H_j^\dagger$, $j = 1, 2, 3$, to it, we find four vectors,

$$\begin{pmatrix} a \\ b \\ 0 \end{pmatrix}, \begin{pmatrix} a+b \\ a+\omega b \\ a+\omega^2 b \end{pmatrix}, \begin{pmatrix} a+\omega^2 b \\ a+b \\ a+\omega b \end{pmatrix}, \begin{pmatrix} a+\omega b \\ a+\omega^2 b \\ a+b \end{pmatrix}. \tag{44}$$

The components of the last three vectors agree, except for permutations. Hence, support size two can occur in three different ways: one component of each vector vanishes if

$$b = -\omega^m a, \qquad m \in \{0, 1, 2\}, \tag{45}$$

holds for some value of m. After removing an irrelevant phase, we obtain the first three vectors given in equation (43). Second, repeating this argument for initial vectors of the form $\psi = (a, 0, b)^T$ and $\psi = (0, a, b)^T$, respectively, leads to the remaining six vectors in (43).

Having exhausted all three-component vectors in the computational basis with support two, we have shown that the nine vectors in (43) are the only states saturating the support inequality (30) for $d = 3$. $\qquad\square$

4.3. Dimensions $d = 5$ and $d = 7$

We will show that it is impossible to reach the lower bound of the support inequality (30) in dimensions $d = 5$ and $d = 7$. The proof relies on a property of the zero distributions of the vectors $H_j^\dagger \psi$, $j = 0 \ldots d$, which were introduced in section 4.1.

Theorem 8. *The additive support uncertainty relation (30) cannot be saturated in dimensions $d = 5$ and $d = 7$.*

Proof. Let $\mathcal{Z}_n^d$ be the set of the zero distributions with n zeroes among the computational-basis coefficients of qudit states in the Hilbert space $\mathcal{H}_d$. These distributions are determined by choosing n out of d indices; hence, there are $|\mathcal{Z}_n^d| = \binom{d}{n}$ such sets. Recalling that *compatible*

sets of zero distributions form equivalence classes, obtained from rigidly shifting a given one, only $|\mathcal{Z}_n^d / \sim | = \binom{d}{n}/d$ *inequivalent* zero distributions exist.

According to theorem 5, a state $|\psi\rangle \in \mathcal{H}_d$ saturating (30) for $d > 3$, must have $n = (d-1)/2$ zeroes in each basis. In addition, a saturating state requires the existence of at least *d incompatible* zero distributions as theorem 6 does not allow compatible zero distributions for more than two bases. In other words, the inequality $|\mathcal{Z}_{(d-1)/2}^d / \sim | \geqslant d$ must hold. Clearly, this does not happen for $d = 5$ and $d = 7$ since $|\mathcal{Z}_2^5 / \sim | = 2 < 5$ and $|\mathcal{Z}_3^7 / \sim | = 5 < 7$, respectively. When $d \geqslant 11$, however, the inequality is satisfied, with $|\mathcal{Z}_5^{11} / \sim | = 42 > 11$, for example.   □

4.4. Numerical results for $5 \leqslant d \leqslant 19$

For prime numbers d greater than seven, more than d incompatible zero distributions exist which removes the bottleneck we exploited to prove theorem 8. In the absence of an analytic handle on the problem, we will use numerical means to check whether the bound imposed by (30) can be reached for dimensions larger than $d = 7$.

A saturating state necessarily has $(d-1)/2$ zeroes in each MU basis. Thus, if one picks two distinct MU bases with labels $j_1, j_2 \in \{0 \ldots d\}$, say, with corresponding zero distributions $\mathcal{Z}^{j_1}$ and $\mathcal{Z}^{j_2}$, the state will have vanishing scalar products with a total of $(d-1)$ states which—in view of corollary 2—are known to be linearly independent. Consequently, there is a *unique* ray $\psi^\perp \in \mathcal{H}_d$ associated with any two zero distributions of the type considered. If the support size of the states $\psi^\perp$ generated in this way (i.e. for all possible choices of initial zero distributions $\mathcal{Z}^{j_1}$ and $\mathcal{Z}^{j_2}$) is always larger than $(d+1)/2$ in some third MU basis, then the support inequality (30) cannot be saturated: if no state with support size $(d+1)/2$ in *three* MU bases exists, then no state with support size $(d+1)/2$ in $(d+1)$ MU bases will exist. Since only a finite number of zero distributions needs to be checked for a given dimension d, this approach actually represents an *algorithm* to check whether the lower bound can be reached.

Running the program for prime numbers with $5 \leqslant d \leqslant 19$ means to check an exponentially increasing number of cases. On a standard PC, the program ran about a second for $d = 5$ and $d = 7$ while it took about a week for $d = 17$. No state has been found which would display $(d-1)/2$ zeroes in three MU bases. For dimensions $d = 5$ and $d = 7$, this result is stronger than that of section 4.3 since the non-existence of a state with two and three zeroes, respectively, is sufficient to derive theorem 8, but not vice versa. Due to the exponential increase in the number of zero distributions, dimensions larger than $d = 19$ were out of reach.

4.5. Dimensions $d > 19$

To satisfy the additive support inequality (30) relative to $(d+1)$ MU bases, a state needs to satisfy more than one pair relation (22) simultaneously which seems unlikely. It is all the more surprising that for dimension $d = 3$ the bound $T(3) = 8$ is actually sharp, i.e. $T_s(3) = T(3)$. Our results for prime dimensions up to $d = 19$ suggest that this case is exceptional.

We conjecture that *the generalised uncertainty relation (30) in prime dimensions can only be saturated when $d = 3$*. Here is a plausibility argument to support this view. Assume that a saturating state $\psi \in \mathcal{H}_d$ exists for some prime dimension $d \geqslant 3$. According to theorem 5, the state must be orthogonal to exactly $(d-1)/2$ vectors from each of the $(d+1)$ MU bases. Corollary 2 implies that orthogonality with respect to just two such sets—i.e. $(d-1)$ vectors— already determines a unique state. Therefore, the remaining $(d-1)^2/2$ vectors (one set of $(d-1)/2$ vectors is associated with each of the $(d-1)$ MU bases not yet considered) must all lie in the same $(d-1)$-dimensional subspace orthogonal to the state ψ. This is known to happen for $d = 3$ but seems hard to satisfy for larger dimensions.

5. Sharp lower bounds

According to the results presented in section 4, no states exist which would saturate the lower bounds (30) for the support sizes in dimensions up to $d = 19$, with the exception of $d = 3$. The focus of this section will be on identifying achievable bounds.

5.1. Dimension $d = 3$

Theorem 7 in section 4.2 displays the states which achieve the lower bound (30) in dimension $d = 3$. In other words, the bound for the overall support of qutrit states ψ is sharp, $\mathcal{S}(3) \geqslant 8$, where $\mathcal{S}(d) \equiv \sum_{j=0}^{d} \|\psi\|_j$ for $\psi \in \mathcal{H}_d$.

5.2. Dimension $d = 5$

Theorem 8 shows that, for any state $\psi \in \mathcal{H}_5$, the overall support of the states $H_j^\dagger \psi$, $j = \{0 \ldots d\}$, must satisfy $\mathcal{S}(5) > 18$. In this section, we will prove a sharp lower bound, namely $\mathcal{S}(5) \geqslant 22 \equiv T_s(5)$.

To begin, we generalise lemma 2 which will be necessary for the proof of lemma 4.

Lemma 3. *Let d be an odd prime and $\omega \equiv e^{\frac{2i\pi}{d}}$. Consider two states $|\phi_{k_1}^{j_1}\rangle, |\phi_{k_2}^{j_2}\rangle \in \mathcal{H}_d$ taken from different standard MU bases, $j_1, j_2 \neq 0$, and let $\{|x\rangle\}$ be the computational basis. Then there can be at most two values of $x \in \{0 \ldots d-1\}$ such that*

$$\langle x | \phi_{k_1}^{j_1} \rangle = \omega^n \langle x | \phi_{k_2}^{j_2} \rangle \tag{46}$$

for the same value of $n \in \{0 \ldots d-1\}$. If two different states are taken from the same basis, $j_1 = j_2$, then the equation has exactly one solution for each value of n.

Proof. See appendix. □

Now consider a state with two vanishing expansion coefficients in both the computational basis and a second basis of the complete set. It turns out that such a state can have only non-zero coefficients in the remaining four bases, resulting in a total support size of 26.

Lemma 4. *If the support of a state $\psi \in \mathcal{H}_5$ equals three in both the computational basis and another standard MU basis with label $j \neq 0$, i.e. $\|\psi\|_0 = \|\psi\|_j = 3$, then its support size in each of the remaining four bases equals five, $\|\psi\|_{j'} = 5$, with $j' \neq 0, j$.*

Proof. The proof, given in the appendix, uses corollary 1 and lemma 3. □

This result allows us to determine a sharp bound $T_s(5)$ for the support size $\mathcal{S}(5)$.

Theorem 9. *Given a state $\psi \in \mathcal{H}_5$, the sharp bound on its overall support size $\mathcal{S}(5)$ in a complete standard set of MU bases is given by $T_s(5) = 22$.*

Proof. To construct the bound, we go through all possible values of the support size of the state ψ in the computational basis, i.e. $\|\psi\|_0 \in \{1 \ldots 5\}$.

For $\|\psi\|_0 = 1$, the pair inequalities (22) imply that the state ψ must have full support in all other five MU bases, i.e. $\|\psi\|_{j \neq 0} = 5$. Hence, the overall support of a computational basis state is given by $\mathcal{S}(5) = 26$.

For $\|\psi\|_0 = 2$, the pair inequalities (22) imply that the state ψ can have at most one zero in each of the other five MU bases, i.e. $\|\psi\|_{j \neq 0} = 4$. Hence, the overall support of ψ is given by $\mathcal{S}(5) = 22$. All 300 states of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\phi_{k_1}^j\rangle - \omega^n |\phi_{k_2}^j\rangle \right), \; j \in \{0 \ldots 5\}, \; k_1, k_2, n \in \{0 \ldots 4\}, \; k_1 \neq k_2 \qquad (47)$$

achieve this bound. More generally, for primes $d > 3$, there are

$$(d+1)\, d \binom{2}{d} = \frac{1}{2} \left(d^2 - 1 \right) d^2 \qquad (48)$$

such states as j takes $(d+1)$ values, n takes d values and there are $\binom{2}{d}$ different pairs of k_1 and k_2. The three-dimensional case is an exception, as demonstrated by theorem 7.

For $\|\psi\|_0 = 3$, the pair inequalities (22) rule out a support size lower than three in any basis from the set. We apply lemma 4: the support size of ψ can equal three in only one other MU basis while the state must have full support in the others, leading to $\mathcal{S}(5) = 26$. It is also possible to have $\|\psi\|_j = 4$ in all bases but the first one, i.e. for $j \neq 0$. In this case seven expansion coefficients would vanish over the complete set, resulting in an overall support size of $\mathcal{S}(5) = 23$. This bound is larger than the one already obtained for the case of $\|\psi\|_0 = 2$.

If $\|\psi\|_0 = 4$ and all other support sizes are also equal to four, the resulting overall support of $\mathcal{S}(5) = 24$ is again larger that the previous bound of $\mathcal{S}(5) = 22$ obtained for $\|\psi\|_0 = 2$. To improve on the value of $\mathcal{S}(5) = 24$, at least one of the other norms must fall below four, i.e. $1 \leqslant \|\psi\|_{j^*} \leqslant 3$ for some $j^* \neq 0$. This assumption, however, sends us back to one of the cases already discussed: we formally map $j^* \mapsto 0$ and repeat the arguments given for $1 \leqslant \|\psi\|_0 \leqslant 3$.

Similarly, full support in all six MU bases cannot beat any of the bounds given so far. Improving on the value of $\mathcal{S}(5) = 30$ is only possible by decreasing some of the support sizes, so that we will end up in one of the previously discussed cases. Having considered all support sizes of a state in a basis, we have exhausted all possibilities and conclude that the bound on the overall support of a state $\psi \in \mathcal{H}_5$ in six MU bases is indeed given by $T_s(5) = 22$. $\qquad \square$

5.3. Dimension $d = 7$

Our aim is to identify states which minimise the overall support $\mathcal{S}(7) = \sum_{j=0}^{7} \|\psi\|_j$. To determine the sharp bound for $d = 7$, we will proceed as in the previous section. However, since no equivalent to lemma 4 is known, we will partly rely on numerical results.

For $\|\psi\|_0 = 1$, the pair inequalities (22) imply that the state ψ must have full support in all other seven MU bases, $\|\psi\|_{j \neq 0} = 7$. Hence, the overall support of ψ is given by $\mathcal{S}(7) = 50$.

For $\|\psi\|_0 = 2$, the pair inequalities (22) imply that the state ψ can have at most one zero in each of the other seven MU bases, i.e. $\|\psi\|_{j \neq 0} = 6$. Hence, the overall support of ψ is given by $\mathcal{S}(7) = 44$, achieved by states of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\phi_{k_1}^j\rangle - \omega^n |\phi_{k_2}^j\rangle \right), \; j \in \{0 \ldots 7\}, \; k_1, k_2, n \in \{0 \ldots 6\}, \; k_1 \neq k_2 . \qquad (49)$$

According to equation (48), there are 1176 such states.

For $\|\psi\|_0 = 3$, the smallest possible value of $\mathcal{S}(7)$ compatible with the pair inequalities is $\mathcal{S}(7) = 38$, as the states in the other bases must have support size at least five each, i.e. $\|\psi\|_{j \neq 0} = 5$. However, no state achieving this bound has been found (numerically). The computations show that a state with support sizes three and five in two MU bases must have full support in the remaining six MU bases so that $\mathcal{S}(7) = 50$. Assuming support size six in all but

Table 1. Lower and sharp bounds $T(d)$ and $T_s(d)$, respectively, on the support sizes of states $\psi \in \mathcal{H}_d$ when expanded in the complete standard set of $(d+1)$ MU bases, for small prime dimensions (numerical results in parentheses).

d	2	3	5	7	11	13	17	19
$T(d)$	9/2	8	18	32	72	98	162	200
$T(d)$ achievable?	$\times$	$\checkmark$	$\times$	$\times$	$(\times)$	$(\times)$	$(\times)$	$(\times)$
$T_s(d)$	5	8	22	(44)	?	?	?	?

the first MU basis, the overall support would be $\mathcal{S}(7) = 45$ which is higher than the bound of $\mathcal{S}(7) = 44$ achievable for $\|\psi\|_0 = 2$.

Given a support size of four in the first MU basis, $\|\psi\|_0 = 4$, not all other support sizes can be equal to four according to theorem 8. One case corresponds a state having support size four in the first and one other MU basis. It is possible to (numerically) construct states for which the remaining six supports sizes must be equal to six, leading to $\mathcal{S}(7) = 44$. We neither know analytic expressions for these states nor their total number. The other scenario compatible with $\|\psi\|_0 = 4$ corresponds to the remaining seven support sizes each equalling five, i.e. $\|\psi\|_{j \neq 0} = 5$, leading to $\mathcal{S}(7) = 39$ but we have obtained no evidence for a state achieving this value.

Assume now that $\|\psi\|_0 = 5$ and that the support of ψ in the other MU bases is also at least five (we exclude all cases with $\|\psi\|_{j^*} < 5$ for some $j^* \neq 0$ since—upon relabeling the MU bases—they have effectively already been considered). An overall support of $\mathcal{S}(7) = 40$ results, below the previously obtained value of $\mathcal{S}(7) = 44$ for $\|\psi\|_0 = 2$. Numerically searching for states achieving this bound, we find that pairs of states with support size five in two MU bases exist but no triples, ruling out the value $\mathcal{S}(7) = 40$. Assuming support size five in two bases and at least six in the remaining six MU bases leads to a higher support size, $\mathcal{S}(7) = 46$.

Starting out with a support size of $\|\psi\|_0 > 5$, no smaller lower bound will exist if all other support sizes take a value of at least six as $\mathcal{S}(7) \geqslant 48$ follows immediately. If not all support sizes take a value of at least six we are being sent back to a previously discussed case. Thus, we have established the sharp bound of $T_s(7) = 44$ on the overall support of seven-component vectors in eight MU bases, partly relying on numerics.

6. Summary and conclusions

Tao's uncertainty relation provides a lower bound on the sum of the support sizes of a state $\psi \in \mathcal{H}_d$ in the standard basis and its Fourier transform, for prime dimensions d. By generalising the bound to arbitrary pairs of MU bases (cf theorem 3), we show in theorem 4 that the sum of the support sizes of a state ψ in a complete standard set of $(d+1)$ MU bases cannot fall below $T(d) \equiv (d+1)^2/2$. The bound is found to be sharp for $d = 3$, and proofs were given that it cannot be saturated for dimensions $d = 2$, 5 and 7. Numerical results indicate that no states exist which achieve the bound for prime numbers up to $d \leqslant 19$. Table 1 summarises these results. We conjecture that the inequality is saturated in dimension $d = 3$ only.

Tao's pair support inequality has been used to identify *KD-nonclassical* states, i.e. states whose Kirkwood–Dirac quasiprobability distribution has negative or complex contributions [10]. Given two orthonormal bases of a finite-dimensional space $\mathcal{H}_d, d \in \mathbb{N}$, with no common elements, a state ψ is found to be KD-nonclassical if the sum of its support sizes in these bases is greater than $(d+1)$. KD-classicality is readily generalised to complete sets of MU bases instead of pairs only. In this context, the results of section 4 mean that no states exist which are

KD-classical with respect to the standard set of $(d+1)$ MU bases in small prime dimensions. When $d = 3$, the claim follows by directly computing the complex KD distributions of the nine minimal uncertainty states of equation (43).

The uncertainty of quantum states involving more than two MU bases has been studied before. Building on a result for a pair of MU observables [33], entropic uncertainty relations have been found which involve $(d+1)$ MU bases [22, 23]. Similarly, Heisenberg's uncertainty relation for continuous variables has a counterpart based on *three* observables satisfying the canonical commutation relation pairwise [18]. Often, the generalisations are straightforward but the resulting inequalities tend not to be achievable. Sharp bounds and the minimising states are usually difficult to find (see e.g. [19, 34] and the review [35]). In this respect, the additive inequality proposed here is no exception.

Support uncertainty relations for multiple MU bases have many interesting features. As for the pair inequalities, a *finite* number of measurements can be sufficient to confirm that a quantum state satisfies a specific bound. The minimum number of required measurements is simply given by the value of the relevant bound, be it sharp or not: it is sufficient that $T(d)$ different outcomes be registered when measurements in the MU bases are performed on the state ψ. This property also ensures that KD-nonclassicality may sometimes be detected with a finite number of measurements.

Furthermore, the lower bounds of support inequalities neither depend on the state considered nor on the value of Planck's constant. The absence of $\hbar$ as a parameter suggests that no support inequalities for continuous variables will emerge in the limit of systems with ever larger dimensions d. The maximal support size of a quantum state grows without bound and, therefore, does not approach a well-defined quantitative measure for uncertainty. Finally, we would like to point out that determining bounds on support sizes is technically difficult since they are basis-dependent quantities.

Establishing sharp bounds for dimensions $d \geqslant 11$ remains an open question which will require new insights since numerical approaches become unfeasible with increasing dimensions. Other directions of future work will be to study support uncertainty relations for smaller sets of MU bases such as triples, for example. The simplification stems from the considerably smaller number of parameters in comparison to complete MU sets. Preliminary analytical and numerical results for small prime dimensions $3 \leqslant d \leqslant 19$ suggest that no state can saturate the bound $T(d;3)$ on the triple uncertainty relation (31) for $d \neq 3$.

Data availability statement

No new data were created or analysed in this study.

Acknowledgments

Appendix

We present proofs of lemma 1, corollary 2 and lemmata 3 and 4, in this order.

Lemma 1. *Let d be an odd prime and $j,k \in \{1\dots d\}$ with $j \neq k$. Then*

$$H_k^\dagger H_j = M(j,k)H_t^\dagger \tag{28}$$

for a monomial matrix $M(j,k)$ if and only if $t = 1 + \chi \in \{1,\dots,d\}$ where the integer χ satisfies $4(j-k)\chi = 1 \mod d$.

Proof. Using equation (14), we calculate the matrix elements of the product $H_k^\dagger H_j$, with $j,k \neq 0$ and $j \neq k$,

$$\left[H_k^\dagger H_j\right]_{\ell\ell'} = \langle\phi_\ell^k|\phi_{\ell'}^j\rangle = \frac{1}{\sqrt{d}}G_d(j-k,\ell-\ell'), \tag{50}$$

with the generalised Gauss sum [36]

$$G_d(j,\ell) = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}\omega^{jx^2+\ell x}. \tag{51}$$

Using $1 = \omega^{(\ell-\ell')^2\chi}\omega^{-(\ell-\ell')^2\chi}$ in (50) and letting χ be an integer satisfying $4(j-k)\chi \equiv 1 \mod d$, we obtain a standard Gauss sum $G_d(j-k,0)$ with known closed form. Explicitly, for $j \neq k$, we obtain

$$\begin{aligned}
G_d(j-k,\ell-\ell') &= \omega^{-(\ell-\ell')^2\chi}\frac{1}{\sqrt{d}}\sum_x\omega^{(j-k)x^2+(\ell-\ell')x}\omega^{(\ell-\ell')^2\chi}\\
&= \omega^{-(\ell-\ell')^2\chi}\frac{1}{\sqrt{d}}\sum_x\omega^{(j-k)\left[x+\overline{2}\,\overline{(j-k)}(\ell-\ell')\right]^2}\\
&= \omega^{-(\ell-\ell')^2\chi}\left[\frac{1}{\sqrt{d}}\sum_x\omega^{(j-k)x^2}\right] = \omega^{-(\ell-\ell')^2\chi}G_d(j-k,0)\\
&= \omega^{-(\ell-\ell')^2\chi}\left(\frac{j-k}{d}\right)\varepsilon_d, \tag{52}
\end{aligned}$$

where $\bar{a}$ denotes the multiplicative inverse of a, $\bar{a}a \equiv 1 \mod d$, while $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol of the integers a and b, and

$$\varepsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \mod 4, \\ i & \text{if } d \equiv 3 \mod 4. \end{cases} \tag{53}$$

The sum $G_d(j-k,\ell-\ell')$ in (52) reduces to a phase factor as it should since the components of the matrix $H_k^\dagger H_j$ are given by the overlap of states stemming from different MU bases.

Combining (50) and (14), we now determine the elements of the matrix $V \equiv H_k^\dagger H_j H_t$ for arbitrary $t \neq 0$:

$$\begin{aligned}
V_{\ell\ell'} &= \sum_{\ell''=0}^{d-1}\langle\phi_\ell^k|\phi_{\ell''}^j\rangle\langle\ell''|\phi_{\ell'}^t\rangle\\
&= \frac{1}{d}\sum_{\ell''=0}^{d-1}G_d(j-k,\ell-\ell'')\omega^{-\ell'\ell''+(t-1)\ell''^2}. \tag{54}
\end{aligned}$$

We can simplify this expression by substituting (52) into it, to find

$$
\begin{aligned}
V_{\ell\ell'} &= \frac{1}{d}\left(\frac{j-k}{d}\right)\varepsilon_d\sum_{\ell''=0}^{d-1}\omega^{-(\ell-\ell'')^2\chi}\omega^{-\ell'\ell''+(t-1)\ell''^2} \\
&= \frac{1}{d}\left(\frac{j-k}{d}\right)\varepsilon_d\omega^{-\ell^2\chi}\sum_{\ell''=0}^{d-1}\omega^{(t-1-\chi)\ell''^2+(2\ell\chi-\ell')\ell''}.
\end{aligned}
\tag{55}
$$

Letting $t = 1 + \chi$, we obtain sums over all dth roots of one which vanish unless the exponents of ω vanish,

$$
\sum_{\ell''=0}^{d-1}\omega^{(2\ell\chi-\ell')\ell''} = \begin{cases} d & \text{if} \quad \ell' = 2\ell\chi \mod d, \\ 0 & \text{otherwise}. \end{cases}
\tag{56}
$$

Thus, for this value of t, the matrix elements of V take the form

$$
V_{\ell\ell'} = \begin{cases} \left(\frac{j-k}{d}\right)\varepsilon_d\omega^{-\ell^2\chi} & \text{if} \quad \ell' = 2\ell\chi \mod d, \\ 0 & \text{otherwise}, \end{cases}
\tag{57}
$$

so that the only non-zero elements of the matrix V are those with indices $(\ell, 2\ell\chi \mod d)$. Each row ℓ has exactly one non-zero entry and the map $\ell \mapsto 2\ell\chi \mod d$ constitutes a permutation of the elements of $\{0\dots d-1\}$ since d is a prime number and $2\chi \neq 0 \mod d$. (Assume this was not the case, i.e. $2\chi x \mod d = 2\chi y \mod d$ for some $x, y \in \{0\dots d-1\}$, $x \neq y$. Then $2\chi(x-y) = nd$ for some integer n which is never the case whenever d is prime and $\chi \neq 0 \mod d$.) As a consequence, each column will also display exactly one non-zero entry.

Therefore, the product V of three Hadamard matrices is equal to a monomial matrix $M(j,k)$ if $t = 1 + \chi$, i.e.

$$
H_k^\dagger H_j = M(j,k)H_{1+\chi}^\dagger.
\tag{58}
$$

We complete the proof by showing that the matrix $V = H_k^\dagger H_j H_t$ is *not* monomial for any other value of t. For $t \neq 1 + \chi$, the sum on the right-hand side of (55) represents another generalised Gauss sum so that

$$
V_{\ell\ell'} = \frac{1}{\sqrt{d}}\left(\frac{j-k}{d}\right)\varepsilon_d\omega^{-\ell^2\chi}G_d(t-1-\chi, 2\ell\chi-\ell')
\tag{59}
$$

with $G_d(t-1-\chi, 2\ell\chi-\ell') = \sqrt{d}\langle\phi_{2\ell\chi}^{1+\chi}|\phi_{\ell'}^t\rangle$. We can now substitute the expression (52) and obtain

$$
V_{\ell\ell'} = \frac{1}{\sqrt{d}}\varepsilon_d^2\left(\frac{j-k}{d}\right)\left(\frac{t-1-\chi}{d}\right)\omega^{-\ell^2\chi}\omega^{-(2\ell\chi-\ell')^2\widetilde{\chi}}
\tag{60}
$$

where $\widetilde{\chi} \in \{1\dots d\}$ is an integer satisfying $4(t-1-\chi)\widetilde{\chi} = 1 \mod d$. Hence, the matrix elements $V_{\ell\ell'}$ are all non-zero confirming that the matrix V is not monomial unless $t = 1 + \chi$. □

An alternative, shorter proof of lemma 1 can be given by representing the Hadamard matrices H_j as 2×2 matrices in $\mathbf{SL}(2, \mathbb{Z}/d\mathbb{Z})$ (cf [37]).

Corollary 2. *Given a complete standard set of MU bases in the space $\mathcal{H}_d$ of prime dimension d, up to d vectors taken from any two MU bases are linearly independent.*

Proof. Construct a matrix M of order $d \times (d_1 + d_2)$ from any $(d_1 + d_2) \leqslant d$ column vectors—expressed in the computational basis—from the two MU bases $\mathcal{B}_{j_1}$ and $\mathcal{B}_{j_2}$. Then left-multiply M by $H_{j_1}^\dagger$. Since $\langle x | H_{j_1}^\dagger | \phi_k^{j_1} \rangle = \langle x | k \rangle$, the first d_1 columns will be elements of the computational basis, while the remaining d_2 columns will be taken from $H_{j_1}^\dagger H_{j_2}$ since $\langle x | H_{j_1}^\dagger | \phi_k^{j_2} \rangle = \langle x | H_{j_1}^\dagger H_{j_2} | k \rangle$. By swapping rows appropriately via a permutation operator P which does not change linear independence of column vectors, the top left square can be mapped to the d_1-dimensional identity. For example, if we consider $d = 5$ and $d_1 = d_2 = 2$, we obtain a 5×4 matrix,

$$PH_{j_1}^\dagger M = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \\ \hline 0 & 0 & * & * \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix}, \tag{61}$$

where the asterisks refer to the elements of $H_{j_1}^\dagger H_{j_2}$.

The $(d_1 + d_2) \leqslant d$ vectors are linearly dependent only if M does *not* have full rank, i.e. $\mathrm{rank}\,(M) < d_1 + d_2$. Since $PH_{j_1}^\dagger$ is unitary, it follows that $\mathrm{rank}\left(PH_{j_1}^\dagger M\right) < d_1 + d_2$. Given the form of the matrix (61), the bottom-right part of $PH_{j_1}^\dagger M$ must contain a $(d_2 \times d_2)$ submatrix with vanishing determinant. However, this is prohibited by corollary 1 which ensures for all prime numbers d that $H_{j_1}^\dagger H_{j_2}$ has non-vanishing minors if $j_1 \neq j_2$. Thus, all $(d_1 + d_2)$ column vectors of M must be linearly independent. $\qquad\square$

Lemma 3. *Let d be an odd prime and $\omega \equiv e^{\frac{2i\pi}{d}}$. Consider two states $|\phi_{k_1}^{j_1}\rangle, |\phi_{k_2}^{j_2}\rangle \in \mathcal{H}_d$ taken from different standard MU bases, $j_1, j_2 \neq 0$, and let $\{|x\rangle\}$ be the computational basis. Then there can be at most two values of $x \in \{0 \ldots d - 1\}$ such that*

$$\langle x | \phi_{k_1}^{j_1} \rangle = \omega^n \langle x | \phi_{k_2}^{j_2} \rangle \tag{46}$$

for the same value of $n \in \{0 \ldots d - 1\}$. If two different states are taken from the same basis, $j_1 = j_2$, then the equation has exactly one solution for each value of n.

Proof. By substituting (13) into (46) and taking the logarithm, one obtains $ax^2 + bx - n = 0$ mod d where $a = j_1 - j_2$ and $b = k_2 - k_1$. This quadratic equation can have no more than two integer solutions. Thus, at most two components of the states $|\phi_{k_1}^{j_1}\rangle$ and $|\phi_{k_2}^{j_2}\rangle$ can be identical in the computational basis, up to multiplication by ω^n. If $j_1 = j_2$, then $a = 0$ and the equation is linear with a single solution for each value of n. $\qquad\square$

Lemma 4. *If the support of a state $\psi \in \mathcal{H}_5$ equals three in both the computational basis and another standard MU basis with label $j \neq 0$, i.e. $\|\psi\|_0 = \|\psi\|_j = 3$, then its support size in each of the remaining four bases equals five, $\|\psi\|_{j'} = 5$, with $j' \neq 0, j$.*

Proof. Four scalar products with the state ψ vanish,

$$\langle x_1 | \psi \rangle = \langle y_1 | \psi \rangle = \langle \phi_{x_2}^j | \psi \rangle = \langle \phi_{y_2}^j | \psi \rangle = 0, \tag{62}$$

two for each of the bases. Hence, the zero distributions of the states ψ and $H_j^\dagger \psi$, are given by $\mathcal{Z}^0 = \{x_1, y_1\}$ and $\mathcal{Z}^j = \{x_2, y_2\}$ respectively, with four integer numbers $x_1, \ldots, y_2 \in \{0 \ldots 4\}$. Now suppose that there is a third MU basis $\mathcal{B}_{j'}$, different from both $\mathcal{B}_0$ and $\mathcal{B}_j$, in which the state ψ does *not* have full support. In other words, there is at least one vanishing scalar product, $\langle \phi_{x_3}^{j'} | \psi \rangle = 0$, say, where $x_3 \in \{0 \ldots 4\}$. Expressing the components of the five vectors

$|x_1\rangle, |y_1\rangle, |\phi_{x_2}^j\rangle, |\phi_{y_2}^j\rangle, |\phi_{x_3}^{j'}\rangle$ with respect to the computational basis and arranging them into a 5×5 matrix, we find, after permuting the rows and rephasing the last three vectors,

$$M = \frac{1}{\sqrt{5}} \begin{pmatrix} \sqrt{5} & 0 & * & * & * \\ 0 & \sqrt{5} & * & * & * \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & \omega^a & \omega^c & \omega^e \\ 0 & 0 & \omega^b & \omega^d & \omega^f \end{pmatrix}, \qquad a, \dots, f \in \{0 \dots 4\}. \qquad (63)$$

Being elements of the Hadamard matrices H_j and $H_{j'}$, the entries of the last three columns are powers of ω, a fifth root of one. Corollary 2 ensures the linear independence of the first four vectors.

If the determinant of M does not vanish, $\det M \neq 0$, then the five column vectors forming it are linearly *independent*, thus spanning $\mathcal{H}_5$. However, the only state being orthogonal to all of $\mathcal{H}_5$ is $\psi = 0$ which does not represent a quantum state. Thus, for an acceptable state ψ producing the given five vanishing expansion coefficients, the five vectors involved must be linearly *dependent*, i.e. $\det M = 0$. Consequently, the determinant of the bottom right 3×3 matrix of M must vanish,

$$\Delta \equiv \det \begin{pmatrix} 1 & 1 & 1 \\ \omega^a & \omega^c & \omega^e \\ \omega^b & \omega^d & \omega^f \end{pmatrix}$$
$$= \omega^{a+d} + \omega^{e+b} + \omega^{c+f} - \omega^{c+b} - \omega^{e+d} - \omega^{a+f} = 0. \qquad (64)$$

Each of the six terms in this expression is a power of a fifth root ω of unity, hence non-zero. It is well known that the set $\{\omega^n \,|\, n = 0, \dots, 3\}$ is linearly independent over the rational numbers $\mathbb{Q}$. As a consequence, every non-zero complex number that is expressible as a linear combination (over $\mathbb{Q}$) of these roots of unity has a unique expression. Since $\omega^4 = -1 - \omega - \omega^2 - \omega^3$, it must follow that the only decomposition of zero over $\mathbb{Q}$ in terms of fifth roots of 1 is $0 = q\left(1 + \omega + \omega^2 + \omega^3 + \omega^4\right)$, with some rational number $q \in \mathbb{Q}$. In other words, for the sum to vanish all five roots must be multiplied to the same rational coefficient.

We distinguish two cases: either $q \neq 0$ or $q = 0$. Since (64) involves six terms with coefficients ± 1, we conclude that the case of $q \neq 0$ cannot be realised: it is impossible to get all five roots to appear with the same non-zero coefficient. For example, let $(a + d) = (e + b) \mod 5$, then equation (64) reduces to

$$\Delta = 2\omega^{a+d} + \omega^{c+f} - \omega^{c+b} - \omega^{e+d} - \omega^{a+f}. \qquad (65)$$

Since all roots must appear, the exponents in (65) are all different. However, the coefficients are not equal throughout and the sum cannot vanish. A similar argument holds for any other equality between exponents.

The case of $q = 0$ must therefore apply: the determinant Δ vanishes if and only if the six terms in equation (64) cancel each other in pairs, i.e. the powers of ω must occur an even number of times, and with an equal number of positive and negative coefficients. Hence, the first term in (64) is necessarily paired up with one of the powers with a negative coefficient leading. Three cases arise which we will consider separately.

(a) For the first and the fourth term to cancel, we must have $(a + d) = (c + b) \mod 5$, or

$$(a - b) = (c - d) \mod 5, \qquad (66)$$

relating the expansion coefficients of two vectors of the *same* basis, namely $|\phi_{x_2}^j\rangle$ and $|\phi_{y_2}^j\rangle$. Consequently, the third and fourth column vectors in the matrix M in (63) have (at least) two equal entries in identical positions, up to an irrelevant common phase factor. This would result in a vanishing 2×2 submatrix of H_j contradicting corollary 1 (and lemma 3). Thus the determinant Δ cannot vanish in this case.

(b) For the first and the fifth term to cancel, we must have $(a + d) = (e + d) \mod 5$, or

$$a = e \mod 5, \tag{67}$$

relating the expansion coefficients of two vectors of *different* bases, namely $|\phi_{x_2}^j\rangle$ and $|\phi_{x_3}^{j'}\rangle$. Corollary 1 does not apply to this case. We do know, however, that the fourth term in the sum (64) must pair up with either the second or the third term of the sum in (64). In the first case, we find $(c + b) = (e + b) \mod 5$, or

$$c = e \mod 5. \tag{68}$$

Given the constraint (67), we we obtain the identity

$$a = c \mod 5, \tag{69}$$

again relating the expansion coefficients of two vectors of the *same* basis, namely $|\phi_{x_2}^j\rangle$ and $|\phi_{y_2}^j\rangle$. As in the Case (a), a contradiction to corollary 1 arises.

In the second case, we pair up terms three and four of the sum (64), leading to the identity $(c + b) = (c + f) \mod 5$, or

$$b = f \mod 5. \tag{70}$$

Together with equation (67), it follows that the last three elements of the third and fifth columns of M are identical. However, according to lemma 3, two vectors stemming from two different bases MU to the computational basis can have at most two identical components.

(c) Assuming that the first and the sixth term of the sum (64) cancel again leads to a contradiction along the lines of the argument considered in Case (b).

Thus, we are forced to conclude that the determinant Δ cannot not vanish for any $j' \neq 0, j$ and any x_3, which implies that the state ψ must have full support. $\qquad\square$

ORCID iDs

Vincenzo Fiorentino ⬤ https://orcid.org/0000-0002-3254-6732
Stefan Weigert ⬤ https://orcid.org/0000-0002-6647-3252

References

[1] Heisenberg W 1927 Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik *Z. Phys.* **43** 172–98
[2] Kennard E H 1927 Zur Quantenmechanik einfacher Bewegungstypen *Z. Phys.* **44** 326–52
[3] Folland G B and Sitaram A 1997 The uncertainty principle: a mathematical survey *J. Fourier Anal. Appl.* **3** 207–38
[4] Donoho D L and Stark P B 1989 Uncertainty principles and signal recovery *SIAM J. Appl. Math.* **49** 906–31
[5] Meshulam R 1992 An uncertainty inequality for groups of order *pq Eur. J. Comb.* **13** 401–7
[6] Wigderson A and Wigderson Y 2021 The uncertainty principle: variations on a theme *Bull. Am. Math. Soc* **58** 225–61

[7] Tao T 2005 An uncertainty principle for cyclic groups of prime order *Math. Res. Lett.* **12** 121–7
[8] Candes E J, Romberg J and Tao T 2006 Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information *IEEE Trans. Inf. Theory* **52** 489–509
[9] Candes E J and Romberg J 2006 Quantitative robust uncertainty principles and optimally sparse decompositions *Found. Comput. Math.* **6** 227–54
[10] De Bièvre S 2021 Complete incompatibility, support uncertainty and Kirkwood–Dirac nonclassicality *Phys. Rev. Lett.* **127** 190404
[11] Kirkwood J G 1933 Quantum statistics of almost classical assemblies *Phys. Rev.* **44** 31–37
[12] Dirac P A M 1945 On the analogy between classical and quantum mechanics *Rev. Mod. Phys.* **17** 195–9
[13] Arvidsson-Shukur D R M, Halpern N Y, Lepage H V, Lasek A A, Barnes C H W and Lloyd S 2020 Quantum advantage in postselected metrology *Nat. Commun.* **11** 3775
[14] Hofmann H F 2011 On the role of complex phases in the quantum statistics of weak measurements *New J. Phys.* **13** 103009
[15] Dressel J and Jordan A N 2012 Significance of the imaginary part of the weak value *Phys. Rev.* A **85** 012107
[16] Arvidsson-Shukur D R M, Drori J C and Halpern N Y 2021 Conditions tighter than noncommutation needed for nonclassicality *J. Phys. A: Math. Theor.* **54** 284001
[17] Kunjwal R, Lostaglio M and Pusey M F 2019 Anomalous weak values and contextuality: robustness, tightness and imaginary parts *Phys. Rev.* A **100** 042116
[18] Kechrimparis S and Weigert S 2014 Heisenberg uncertainty relation for three canonical observables *Phys. Rev.* A **90** 062118
[19] Kechrimparis S and Weigert S 2017 Geometry of uncertainty relations for linear combinations of position and momentum *J. Phys. A: Math. Theor.* **51** 025303
[20] Dodonov V V, Kurmyshev E V and Man'ko V I 1980 Generalized uncertainty relation and correlated coherent states *Phys. Lett.* A **79** 150–2
[21] Dodonov V V 2018 Variance uncertainty relations without covariances for three and four observables *Phys. Rev.* A **97** 022105
[22] Ivanović I D 1992 An inequality for the sum of entropies of unbiased quantum measurements *J. Phys. A: Math. Gen.* **25** L363–4
[23] Sánchez J 1993 Entropic uncertainty and certainty relations for complementary observables *Phys. Lett.* A **173** 233–9
[24] Ballester M A and Wehner S 2007 Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases *Phys. Rev.* A **75** 022319
[25] Rényi A 1961 On measures of entropy and information *Proc. 4th Berkeley Symp. on Mathematical Statistics and Probability* vol 1 pp 547–61
[26] Stevenhagen P and Lenstra H W 1996 Chebotarëv and his density theorem *Math. Intell.* **18** 26–37
[27] Frenkel P E 2004 Simple proof of Chebotarëv's theorem on roots of unity (arXiv:math/0312398)
[28] Ivanović I D 1981 Geometrical description of quantal state determination *J. Phys. A: Math. Gen.* **14** 3241–5
[29] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements *Ann. Phys., NY* **191** 363–81
[30] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases *Algorithmica* **34** 512–28
[31] Durt T 2005 About mutually unbiased bases in even and odd prime power dimensions *J. Phys. A: Math. Gen.* **38** 5267–83
[32] Bruzda W, Tadej W and Życzkowski K 2006 Catalogue of complex Hadamard matrices (available at: https://chaos.if.uj.edu.pl/~karol/hadamard/)
[33] Maassen H and Uffink J B M 1988 Generalized entropic uncertainty relations *Phys. Rev. Lett.* **60** 1103–6
[34] Wu S, Yu S and Mølmer K 2009 Entropic uncertainty relation for mutually unbiased bases *Phys. Rev.* A **79** 022104
[35] Wehner S and Winter A 2010 Entropic uncertainty relations—a survey *New J. Phys.* **12** 025009
[36] Berndt B C, Williams K S and Evans R J 1998 *Gauss and Jacobi Sums* (New York: Wiley)
[37] Neuhauser M 2002 An explicit construction of the metaplectic representation over a finite field *J. Lie Theory* **12** 15–30