All classes of informationally complete symmetric measurements in finite dimensions

Katarzyna Siudzińska
Institute of Physics, Faculty of Physics, Astronomy and Informatics
Nicolaus Copernicus University in Toruń, ul. Grudziądzka 5, 87-100 Toruń, Poland

A broad class of informationally complete symmetric measurements is introduced. It can be understood as a common generalization of symmetric, informationally complete POVMs and mutually unbiased bases. Additionally, it provides a natural way to define two new families of mutually unbiased symmetric measurement operators in any finite dimension. We show a general method of their construction, together with an example of an optimal measurement. Finally, we analyze the properties of symmetric measurements and provide applications in entropic relations and entanglement detection.

1. INTRODUCTION

Quantum measurements are important tools in quantum information processing for obtaining information about quantum states. In quantum information theory, measurements are represented by a collection of positive operator-valued measures (POVMs); that is, positive semidefinite operators that sum up to the identity operator. Measurements are informationally complete if they allow for a full tomography of a quantum state [1]. In particular, if the Hilbert space of a quantum system is $d$-dimensional, then a complete information about the state is obtained from the expectation values of $d^2$ operators spanning the $d^2$-dimensional space of observables.

Through the introduction of symmetries between the measurement operators, one recovers two important classes of projective measurements. A symmetric, informationally complete (SIC) POVM consists in $d^2$ elements such that every operator inner product between different pairs is the same $[2]$. Mutually unbiased bases (MUBs) are (at most) $d+1$ sets of $d$ orthogonal projectors where the transition probability between any two states from different bases is constant $[3, 4]$. Interestingly, SIC POVMs and MUBs have many common applications, including quantum state tomography $[5, 6]$, quantum key distribution $[7, 8]$, and quantum entanglement detection $[9, 10]$. They are also often analyzed in the same context $[11–14]$. This indicates that the two objects are closely related.

In this paper, we show that SIC POVMs and MUBs are special cases of a more general concept: collections of mutually unbiased symmetric measurements that form an informationally complete set. Further analysis reveals that there are indeed two more classes of such measurements in every finite dimension. We provide a general method of construction as well as an example of optimal measurement with projective operators of rank 2. Possible applications are discussed in entropic uncertainty relations and quantum entanglement detection.

Our results indicate that symmetric measurements have the ability to become just as versatile in their applications in both theoretical and experimental physics as SIC POVMs, MUBs, and their non-projective generalizations. For one, symmetric measurements can be used in quantum entanglement to formulate enhanced separability criteria $[15]$ and construct indecomposable entanglement witnesses $[16]$. In quantum cryptography, they may be applied to design quantum key distribution protocols with improved error and noise tolerance $[17]$. Projective informationally complete symmetric measurements may provide examples of quantum 2-designs $[18]$, which are used for optimal quantum state estimation in quantum tomography. From a mathematical perspective, it might be possible to find analogues in the finite geometry between all classes of projective symmetric measurements. This could shed some light on the existence of maximal sets of MUBs and SIC POVMs in any dimension. On the other hand, non-projective measurements find applications in post processing tasks, like error rate estimation and error correction. Their advantage comes from preserving partial information about the measured state, including correlations with other subsystems.

2. SYMMETRIC MEASUREMENTS

Consider a collection of $N$ POVMs, where each of them is $M$-elemental. Let us call this collection an $(N, M)$-POVM and denote its elements by $E_{a,k}$, with the index range $a = 1, \ldots, N$ and $k = 1, \ldots, M$. Now, we impose the symmetry conditions on the inner products of operators within the same POVM as well as between different POVMs. This leads to the following set of relations.

**Definition 1.** An $(N, M)$-POVM is a set of $N$ POVMs $\{E_{a,k}; k = 1, \ldots, M\}$ that satisfy the symmetry conditions

\[
\begin{align*}
\text{Tr}(E_{a,k}) &= w, \\
\text{Tr}(E_{a,k}^2) &= x, \\
\text{Tr}(E_{a,k}E_{a,\ell}) &= y, \quad \ell \neq k, \\
\text{Tr}(E_{a,k}E_{\beta,\ell}) &= z, \quad \beta \neq \alpha.
\end{align*}
\]

In Appendix A it is shown that this definition implies that

\[
w = \frac{d}{M}, \quad y = \frac{d-Mx}{M(M-1)}, \quad z = \frac{d}{M^2},
\]

and $x$ is a free parameter from the range

\[
\frac{d}{M^2} < x \leq \min \left\{ \frac{d^2}{M^2}, \frac{d}{M} \right\}.
\]
If $x = d^2/M^2$, then the POVMs are projective measurements. On the other hand, $x = d/M^2$ corresponds to $E_{\alpha,k} = \mathbb{I}_d/M$. Note that eq. (4) implies that it is not always possible to obtain projective measurements from our symmetric construction.

**Remark 1.** There are no projective $(N, M)$-POVMs for $M < d$.

The $(N, M)$-POVM is informationally complete if and only if it contains $d^2$ linearly independent elements. For every $M$-elemental POVM numbered by the index $\alpha$, there are $M - 1$ linearly independent operators due to the constraint $\sum_{k=1}^{M} E_{\alpha,k} = \mathbb{I}_d$. Collectively, all POVMs share the final spanning operator, which is the identity $\mathbb{I}_d$. Therefore, $M$ and $N$ are related via $(M - 1)N = d^2 - 1$. Provided that this condition holds, the set of operators $\{E_{\alpha,k}\}$ is indeed informationally complete (see Appendix B). Any state $\rho$ can be decomposed into

$$\rho = \sum_{\alpha=1}^{N} \sum_{k=1}^{M} p_{\alpha,k} F_{\alpha,k}, \quad (4)$$

where $p_{\alpha,k} = \text{Tr}(E_{\alpha,k}\rho)$ are the probability outcomes and

$$F_{\alpha,k} = \frac{1}{x - y} \left( E_{\alpha,k} - \frac{(N - 1)z + y}{Nw} \mathbb{I}_d \right). \quad (5)$$

Up until this point, our construction could be seen as nothing more than a common generalization of SIC POVMs and MUBs. Actually, the above considerations introduce in fact a unified method to describe general SIC POVMs \[19, 20\] and mutually unbiased measurements (MUMs) \[21\], which respectively generalize the notions of SIC POVMs and MUBs to nonprojective measurements. However, these provide only two special cases of $(N, M)$-POVMs. Further observations can be made based on the relation

$$(M - 1)N = d^2 - 1, \quad (6)$$

which determines the decomposition of $d^2 - 1$ linearly independent operators (without the identity) into $N$ POVMs with $M$ elements each. For $d = 2$, there are indeed only two possible choices: $(N = 1, M = 4)$ for the general SIC POVM and $(N = 3, M = 2)$ for MUMs. However, for any finite $d > 2$, there exist four decompositions of $d^2 - 1$ in terms of $N$ and $M$, and therefore four families of $(N, M)$-POVMs.

**Proposition 1.** In any finite dimension $d$, there exist at least four informationally complete $(N, M)$-POVMs. The allowed choices of $M$ and $N$ are as follows:

(i) $M = d^2$ and $N = 1$ (general SIC POVM),

(ii) $M = d$ and $N = d + 1$ (MUMs),

(iii) $M = 2$ and $N = d^2 - 1$,

(iv) $M = d + 2$ and $N = d - 1$.

There can be, of course, more choices of $M$ and $N$, depending on the number of divisors for $d^2 - 1$. For example, for the first non-trivial case of $d = 5$, one has two additional choices besides the standard four; namely, $(N = 8, M = 4)$ and $(N = 3, M = 9)$.

### 3. CONSTRUCTION METHOD

By following the procedure introduced by Kalev and Gour \[20, 21\], we provide a general method of constructing any informationally complete $(N, M)$-POVM. Let us take an orthonormal Hermitian operator basis $\{G_0 = \mathbb{I}_d/\sqrt{d}, G_{\alpha,k}; \alpha = 1, \ldots, N, k = 1, \ldots, M - 1\}$ with traceless $G_{\alpha,k}$. Next, construct $MN$ operators

$$H_{\alpha,k} = \begin{cases} G_\alpha - \sqrt{M}(\sqrt{M} + 1)G_{\alpha,k}, & k = 1, \ldots, M - 1, \\ \sqrt{M}G_\alpha, & k = M, \end{cases} \quad (7)$$

where $G_\alpha = \sum_{k=1}^{M-1} G_{\alpha,k}$. The elements of $(N, M)$-POVMs are given by

$$E_{\alpha,k} = \frac{1}{M} \mathbb{I}_d + tH_{\alpha,k}. \quad (8)$$

The parameter $t$, which is chosen in such a way that $E_{\alpha,k} \geq 0$, belongs to the range

$$-\frac{1}{M} \frac{1}{\lambda_{\text{max}}} \leq t \leq \frac{1}{M} \frac{1}{\lambda_{\text{min}}}, \quad (9)$$

where $\lambda_{\text{max}}$ and $\lambda_{\text{min}}$ are the minimal and maximal eigenvalue from among all eigenvalues of $H_{\alpha,k}$, respectively. This construction guarantees that eqs. (1) and (2) defining the $(N, M)$-POVM are satisfied.

The relation between $x$ and $t$ is provided by the formula

$$x = \frac{d}{M^2} + t^2(M - 1)(\sqrt{M} + 1)^2. \quad (10)$$

Note that if $E_{\alpha,k}$ is positive for a given value of $x$, then it is also positive for any $x' \in (d/M^2, x)$. Therefore, one is usually interested in determining the optimal value $x_{\text{opt}}$ of $x$. Coincidentally, $x_{\text{opt}}$ depends on the choice of $G_{\alpha,k}$. The closer this parameter is to $d^2/M^2$, the closer the associated POVM is to a projective measurement. If $x_{\text{opt}}$ reaches the upper bound of $x$, then the corresponding $(N, M)$-POVM is called optimal. Examples include the SIC POVMs and mutually unbiased bases.

Conversely, given an $(N, M)$-POVM, one recovers the Hermitian basis

$$G_{\alpha,k} = \frac{1}{tM(\sqrt{M} + 1)^2}\left[ \mathbb{I}_d + \sqrt{M}E_{\alpha,M} - \sqrt{M}(\sqrt{M} + 1)E_{\alpha,k} \right]. \quad (11)$$

The correspondence between $G_{\alpha,k}$ and $E_{\alpha,k}$ is one-to-one. Given any orthonormal Hermitian operator basis that consists in all traceless operators and the identity, one can
always construct a corresponding \((N, M)\)-POVM. Moreover, any \((N, M)\)-POVM can be obtained through this method.

Observe that in general it is not easy to find the relation between two different \((N, M)\)-POVMs. However, the problem simplifies significantly for a special case where \((N' = M - 1, M' = N + 1)\). This is true e.g. for the pairs (i)-(iii) and (ii)-(iv) from Proposition 11. Then, the \((N, M)\)-POVM and the \((N', M')\)-POVM can be both constructed using the same orthonormal basis provided that \(G_{α', k'} = G_{k, α}\). This observation indicates that there might be a closer relation between the aforementioned families of \((N, M)\)-POVMs than between SIC POVMs and MUBs.

4. EXAMPLE – OPTIMAL POVMs

Let us provide one more example of an optimal informationally complete \((N, M)\)-POVM; that is, a measurement for which the free parameter \(x\) reaches its upper bound. Consider the special case with \(N = d^2 - 1\) and \(M = 2\). Using eqs. (7) and (8), one finds the formula for the measurement operators

\[
E_{α, k} = \frac{1}{2} I_d + t(-1)^k(1 + \sqrt{2})G_α, \tag{12}
\]

where \(G_α\) are the traceless Hermitian basis operators. From eq. (10), we see that the upper bound \(x = d/2\) corresponds to

\[
|t| = \frac{\sqrt{d}}{2(\sqrt{2} + 1)}. \tag{13}
\]

Moreover, \(|t| = 1/|2\lambda|\), where \(λ\) is the eigenvalue of \(H_{α, k} = (-1)^k(1 + \sqrt{2})G_α\) with the greatest module. Therefore, an extremal eigenvalue of the corresponding \(G_α\) is \(±1/\sqrt{d}\). A good example of such basis is the tensor product of Pauli matrices \(G_{d+i+j} = σ_i ⊗ σ_j\) in \(d = 4\), where \(σ_0 = I_2/\sqrt{2}\) and

\[
σ_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad σ_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad σ_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{14}
\]

Then, the \((3, 2)\)-POVM elements, given by

\[
E_α = \frac{1}{2} I_4 ± G_α, \tag{15}
\]

are rank-2 projectors, as \(E_{α}^2 = E_α\) have two non-vanishing eigenvalues.

5. APPLICATIONS

5.1. Entropic relations

Although uncertainty relations were first formulated with variance, they can be alternatively expressed in terms of entropy. With the development of quantum information theory, they found new applications in quantum cryptography \[22, 23\], quantum entanglement \[24, 25\], and non-locality \[26\].

To derive entropic uncertainty relations for \((N, M)\)-POVMs, we first find the index of coincidence. It is defined as a sum of squared probabilities \[12\],

\[
C = \sum_{α=1}^{N} \sum_{k=1}^{M} p_{α, k}^2, \tag{15}
\]

where in our case \(p_{α, k} = Tr(ρE_{α, k})\).

**Lemma 1.** Let \(\{E_{α, k}; α = 1, \ldots, N; k = 1, \ldots, M\}\) be an informationally complete \((N, M)\)-POVM characterized by the parameter \(x\). For an arbitrary state \(ρ\), the index of coincidence \(C\) is upper bounded by

\[
\tilde{C} = \frac{d - 1 - d^2 + M^2x}{d M(M - 1)}. \tag{16}
\]

For a detailed proof, as well as an exact expression for \(C\), refer to Appendix C. Observe that for optimal projective \((N, M)\)-POVMs, where \(x = d^2/M^2\), the index of coincidence obeys a simpler condition,

\[
C ≤ \frac{2d(d - 1)}{M(M - 1)}. \tag{17}
\]

In this case, the greater the value of \(M\), the tighter the upper bound.

Now, using Lemma 1 we obtain the entropic uncertainty relations (proof in Appendix D)

\[
\frac{1}{N} \sum_{α=1}^{N} H(E_{α, ρ}) ≥ \ln \frac{N}{C}, \tag{18}
\]

for the Shannon entropy \(H(E_{α, ρ}) = -\sum_{k=1}^{M} p_{α, k} \ln p_{α, k}\) associated with the measurement \(E_{α} = \{E_{α, k}; k = 1, \ldots, M\}\). The special cases agree with the entropic relations for mutually unbiased bases \[24, 25\] and measurements \[24\] as well as SIC POVMs \[12\] and their generalization \[30\].

5.2. Entanglement detection

Quantum entanglement is a key feature in quantum theory. It provides important resources for modern quantum technologies, such as quantum cryptography \[31\], quantum teleportation \[32\], and quantum computation \[33\]. An important problem is to distinguish between separable and entangled states.

Consider a bipartite quantum state \(ρ\) of the composite system with the underlying Hilbert space \(H = H_A ⊗ H_B\), where \(dim H_A/B = d_A/B\). On each subsystem, we choose an \((N_A/B, M_A/B)\)-POVM and denote it by \(\{E_{α, A/B}\}\). Linear correlations between \(\{E_{α, k}\}\) and \(\{E_{β, α, k}\}\) are encoded in the matrix

\[
P_{α, k, β, ℓ} = Tr[μ(E_{α, k} ⊗ E_{β, ℓ})]. \tag{19}
\]
Using this matrix and Lemma 1, we construct the following separability criterion.

**Proposition 2.** If a bipartite state $\rho$ is separable, then

$$
\|P\|_{tr} \leq \sqrt{C_A C_B},
$$

(20)

where $C_{A/B}$ is the upper bound for the index of coincidence that characterizes the $(N_{A/B}, M_{A/B})$-POVM.

The proof is presented in Appendix E. For SIC POVMs, one recovers the ESIC criterion \[10\].

Now, consider a special case where $d_A = d_B = d$. Take two $(N, M)$-POVMs characterized by the same parameter $x$. Then, it is possible to formulate yet another separability criterion. Namely, if $\rho$ is a bipartite separable state, then (see Appendix E)

$$
Tr(P) \leq \tilde{C}. \tag{21}
$$

Due to $Tr(P) \leq \|P\|_{tr}$, this criterion detects more separable states than eq. (20). Moreover, it includes other popular separability criteria based on MUBs \[9\], MUMs \[34\], and general SIC POVMs \[35\].

6. CONCLUSIONS

In this paper, we proposed the most general class of symmetric measurements that are mutually unbiased, which we call $(N, M)$-POVMs to underline the number and type of measurement operators. In particular, we found that there exist at least four informationally complete symmetric measurements in any finite dimension, including general SIC POVMs and mutually unbiased measurements. We provided a method to construct $(N, M)$-POVMs from Hermitian operator bases as well as an example of optimal measurement in dimension $d = 4$. Finally, we presented possible applications in entropic uncertainty relations and entanglement detection by introducing two separability criteria.

An important open question is the existence of optimal measurements in any dimension. In other words, is it always possible to construct measurements with the maximal value of $x$. The answer is not known for MUBs nor SIC POVMs despite extensive research. A simpler task is to find optimal $(N, M)$-POVMs for the two newly introduced classes. Note that our construction can be further generalized in a manner similar to the introduction of semi-SIC POVMs \[36\]. Also, it is interesting how informationally complete symmetric measurements can be applied more efficiently than MUBs and SIC POVMs in quantum state tomography, post processing tasks, and entanglement detection.

7. ACKNOWLEDGEMENTS

This paper was supported by the Foundation for Polish Science (FNP) and the Polish National Science Centre project No. 2018/30/A/ST2/00837.
(1993).
[33] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001).
[34] B. Chen, T. Ma, and S.-M. Fei, Phys. Rev. A 89, 064302 (2014).
[35] B. Chen, T. Li, and S.-M. Fei, Quant. Inf. Proc. 14, 2281–2290 (2015).
[36] I. J. Geng, K. Golubeva, and G. Gour, Phys. Rev. Lett. 126, 100401 (2021).
[37] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. 60, 1103 (1988).

Appendix A: Parameter values for symmetric measurements

All elements of a POVM sum up to identity. We use this to show that the values of \( w \) and \( z \) follow directly from the definition, as

\[ d = \text{Tr}(\mathbb{I}_d) = M \sum_{\alpha=1}^{M} \text{Tr}(E_{\alpha, k}) = Mw \]  
(A1)

and

\[ w = \text{Tr}(E_{\alpha, k}) = M \sum_{\alpha=1}^{M} \text{Tr}(E_{\alpha, k}E_{\beta, \ell}) = Mz. \]  
(A2)

To obtain the formula for \( y \), we compute

\[ w = \text{Tr}(E_{\alpha, k}) = \sum_{\ell=1}^{M} \text{Tr}(E_{\alpha, k}E_{\beta, \ell}) = x + (M-1)y. \]  
(A3)

The range of \( x \) is determined in two steps. First, we note that the measurement operators range from rescaled rank-1 projectors to rescaled identity operators. Hence, the upper bound is \( x = w^2 \) and the lower bound is \( x = w^2/d \). Alternatively, the lower bound follows from the Cauchy-Schwarz inequality \( \text{Tr}(E_{\alpha, k}) = (\text{Tr}E_{\alpha, k}\mathbb{I}_d) < \sqrt{dM} \), where the sharp inequality discards the case with all \( E_{\alpha, k} = \mathbb{I}_d/M \).

Next, one must have \( y \geq 0 \) because otherwise \( E_{\alpha, k} \neq 0 \). This imposes an additional condition on \( x \),

\[ x \leq \frac{d}{M}, \]  
(A4)

which is stronger than \( x \leq w^2 = d^2/M^2 \) whenever \( M < d \).

Appendix B: Proof of informational completeness

Let us take \( d^2 - 1 \) real numbers \( r_{\alpha, k} \) such that

\[ \sum_{\alpha=1}^{N} \sum_{k=1}^{M-1} r_{\alpha, k} E_{\alpha, k} = 0. \]  
(B1)

The \((N, M)\)-POVM is informationally complete if its operators \( E_{\alpha, k} \) with \( \alpha = 1, \ldots, N \) and \( k = 1, \ldots, M-1 \) form a linearly independent set; that is, if eq. (B1) implies that \( r_{\alpha, k} = 0 \). By calculating the trace of eq. (B1), we find that

\[ \text{Tr} \left( \sum_{\alpha=1}^{N} \sum_{k=1}^{M-1} r_{\alpha, k} E_{\alpha, k} \right) = w \sum_{\alpha=1}^{N} \sum_{k=1}^{M-1} r_{\alpha, k} = 0. \]  
(B2)

Next, we multiply eq. (B1) by \( E_{\beta, \ell} \) with an arbitrary \( \beta \) before taking the trace. Using eq. (B2), one obtains

\[ \text{Tr} \left( \sum_{\alpha=1}^{N} \sum_{k=1}^{M-1} r_{\alpha, k} E_{\alpha, k} E_{\beta, \ell} \right) = (x - y)r_{\beta, \ell} + (y - z) \sum_{k=1}^{M-1} r_{\beta, k} = 0 \]  
(B3)

for \( \ell = 1, \ldots, M - 1 \), as well as

\[ \text{Tr} \left( \sum_{\alpha=1}^{N} \sum_{k=1}^{M-1} r_{\alpha, k} E_{\alpha, k} E_{\beta, M} \right) = (y - z) \sum_{k=1}^{M-1} r_{\beta, k} = 0. \]  
(B4)

Taking \( z = y \) results in \( x = d/M^2 \), which lies outside the domain of \( x \). Therefore, the solution of eq. (B4) is

\[ \sum_{k=1}^{M-1} r_{\beta, k} = 0. \]  
(B5)

If we input this result into eq. (B3), it follows that

\[ (x - y)r_{\beta, \ell} = 0, \quad \ell = 1, \ldots, M - 1. \]  
(B6)

Coincidentally, \( y = x \) also gives \( x = d/M^2 \) that is not an admissible value. At last, the only solution of eq. (B1) is \( r_{\beta, \ell} = 0 \), and hence the set \( \{ E_{\alpha, k} | \alpha = 1, \ldots, N; k = 1, \ldots, M-1 \} \) indeed consists in linearly independent operators.

Appendix C: Index of coincidence

Recall that any quantum state can be expanded into

\[ \rho = \sum_{\alpha=1}^{N} \sum_{k=1}^{M} p_{\alpha, k} F_{\alpha, k} \]  
(C1)

using the probability distributions \( p_{\alpha, k} = \text{Tr}(\rho E_{\alpha, k}) \) and the operators \( F_{\alpha, k} \) given in eq. (C). Now, let us calculate

\[ \text{Tr}(\rho^2) = \sum_{\alpha, \beta=1}^{N} \sum_{k, \ell=1}^{M} p_{\alpha, k} p_{\beta, \ell} \text{Tr}(F_{\alpha, k} F_{\beta, \ell}). \]  
(C2)

From definition, it follows that

\[ \text{Tr}(F_{\alpha, k} F_{\beta, \ell}) = \frac{1}{(x - y)^2} \left[ \text{Tr}(E_{\alpha, k} E_{\beta, \ell}) + A(dA - 2w) \right]. \]  
(C3)
where for simplicity we introduced a new symbol
\[ A = \frac{(N - 1)z + y}{N w}. \quad (C4) \]
This allows us to rewrite eq. (C2) into
\[
\text{Tr}(\rho^2) = \frac{1}{(x - y)^2} \left[ \sum_{\alpha=1}^{N} \sum_{k=1}^{M} p_{\alpha,k} \text{Tr}(E_{\alpha,k}^2) + \sum_{\alpha=1}^{N} \sum_{k=1}^{M} \sum_{\ell \neq k} p_{\alpha,k} p_{\alpha,\ell} \text{Tr}(E_{\alpha,k}E_{\alpha,\ell}) + N^2 A (dA - 2w) \right] = \frac{1}{(x - y)^2} \left[ C x + (N - C) y + N (N - 1) z \right] + N^2 A (dA - 2w) = \frac{d M (M - 1) C - d^3 - M^2 x}{d (M^2 x - d)}.
\]
It is straightforward to solve this equation in terms of \( C \).
One gets
\[ C = \frac{d (M^2 x - d) \text{Tr}(\rho^2) + d^3 - M^2 x}{d (M^2 - 1)}, \quad (C5) \]
which is the exact (state-dependent) formula for the index of coincidence. The upper bound follows from \( \text{Tr}(\rho^2) \leq 1 \).

**Appendix D: Entropic uncertainty relations**

Our goal is to compute the Shannon entropy
\[ H(\mathcal{E}_\alpha, \rho) = -\sum_{k=1}^{M} p_{\alpha,k} \ln p_{\alpha,k} \quad (D1) \]
averaged over all measurements \( \mathcal{E}_\alpha \). It has been shown that for any probability distribution \[28, 37\]
\[ \sum_{k=1}^{M} p_{\alpha,k} \ln p_{\alpha,k} \leq \ln \sum_{k=1}^{M} p_{\alpha,k}^2, \quad (D2) \]
Hence, from the concavity of the logarithm function, one obtains
\[ \frac{1}{N} \sum_{\alpha=1}^{N} H(\mathcal{E}_\alpha, \rho) \geq -\frac{1}{N} \sum_{\alpha=1}^{N} \ln \sum_{k=1}^{M} p_{\alpha,k}^2 \geq -\ln \left[ \frac{1}{N} \sum_{\alpha=1}^{N} \sum_{k=1}^{M} p_{\alpha,k}^2 \right] = \ln \frac{N}{C}, \]
where \( C \) is the index of coincidence.

**Appendix E: Separability criterion**

Proposition 2 can be proven analogically to the ESIC criterion in ref. \[10\]. For a product state \( \rho = \rho_A \otimes \rho_B \), the elements of the \( P \) matrix are simply
\[ P_{\alpha, k; \beta, \ell} = \text{Tr}(\rho_A E_{\alpha,k}^A) \text{Tr}(\rho_B E_{\beta,\ell}^B) = P_{\alpha, k}^A P_{\beta, \ell}^B. \quad (E1) \]
The trace norm reads
\[ \|P\|_{tr} = \text{Tr} \sqrt{P^2} = \sqrt{\sum_{\alpha, \beta = 1}^{N} \sum_{k, \ell = 1}^{M} P_{\alpha, k; \beta, \ell}} \leq \sqrt{C_A C_B}, \quad (E2) \]
with \( C_{A/B} \) being the upper bound for the index of coincidence associated with \( \rho_{A/B} \). From the convexity of the trace norm, this condition follows for an arbitrary separable state.

**Appendix F: Separability criterion 2**

Again, we prove the condition for a product state \( \rho = \rho_A \otimes \rho_B \) and extend the end result to all separable states using linearity of trace. Starting from eq. (E1), we write
\[ \text{Tr} P = \sum_{\alpha=1}^{N} \sum_{k=1}^{M} P_{\alpha, k; \alpha, k} = \sum_{\alpha=1}^{N} \sum_{k=1}^{M} p_{\alpha,k}^A p_{\alpha,k}^B \leq \frac{1}{2} \sum_{\alpha=1}^{N} \sum_{k=1}^{M} \left[ (p_{\alpha,k}^A)^2 + (p_{\alpha,k}^B)^2 \right] = \frac{1}{2} (C_A + C_B) \leq \tilde{C}. \quad (F1) \]
In the above derivation, we used the inequality of arithmetic and geometric means
\[ \frac{1}{N} \sum_{k=1}^{N} x_k \geq \left( \prod_{k=1}^{N} x_k \right)^{1/N}. \quad (F2) \]