Entropic uncertainty relation for mutually unbiased bases

Shengjun Wu (吴盛俊),[1,2] Sixia Yu (郁司夏),[2,3] and Klaus Mølmer[1]

[1]*The Lundbeck Foundation Theoretical Center for Quantum System Research, Department of Physics and Astronomy, Aarhus University, Aarhus, Denmark*

[2]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Centre for Quantum Technologies and Physics Department, National University of Singapore, 2 Science Drive 3, Singapore 117542*

(Received 21 November 2008; published 5 February 2009)

We derive inequalities for the probabilities of projective measurements in mutually unbiased bases of a qudit system. These inequalities lead to wider ranges of validity and tighter bounds on entropic uncertainty inequalities previously derived in the literature.

DOI: 10.1103/PhysRevA.79.022104   PACS number(s): 03.65.Ta, 03.67.Mn, 03.65.Ud

I. INTRODUCTION

Heisenberg's position-momentum uncertainty relation led to Bohr's introduction of the complementarity principle, which limits the joint measurability, or knowability, of different properties of a physical system. Complementarity is profoundly linked with the Copenhagen interpretation of quantum theory, according to which it poses limitations on a physical system's ability to manifest certain physical properties and, hence, on the meaning of physical reality of these properties. At a more quantitative level, the nonexistence of a basis for a Hilbert space whose basis states are simultaneous eigenstates of two noncommuting observables leads to a formal relationship between statistical predictions possible for measurement outcomes of such observables on a quantum system. The standard deviations of any two Hermitian operators Ω_1 and Ω_2 on a finite-dimensional system Hilbert space, defined as $\Delta\Omega_i = \sqrt{\langle\Omega_i^2\rangle - \langle\Omega_i\rangle^2}$, obey the Robertson-Schrödinger uncertainty inequality $\Delta\Omega_1\Delta\Omega_2 \geqslant \frac{1}{2}\sqrt{|\langle[\Omega_1,\Omega_2]\rangle|^2 + |\langle\{(\Omega_1-\langle\Omega_1\rangle),(\Omega_2-\langle\Omega_2\rangle)\}\rangle|^2}$. The inequality with only the commutator term is due to Robertson [1], while the tighter bound with the anticommutator term included was given by Schrödinger [2]. Quantum theory is applied to provide theoretical predictions in the form of expectation values, and quantum-mechanical uncertainties play an important role both in the comparison between theory and experiments and in the assessment of the possible use of simpler, e.g., semiclassical, theoretical methods.

In quantum information theory, complementarity and quantum-mechanical uncertainty are central concepts because they provide the ultimate limits on how much information can be extracted by measurements on a physical system. Thus, on the one hand, the uncertainty relation quantitatively limits the achievements of computing and communication systems, and on the other hand, it provides security against adversary attacks on a secret communication system. In quantum information theory it is not the magnitude of physical observables that is of interest, but to a much larger extent binary values corresponding to the identification of a state being occupied with zero or unit occupancy. When projective measurements are carried out to determine if a quantum system is in a particular basis state, the resulting average population is identified as a weighted sum of the measurement outcomes zero and unity, and since the projection operators on nonorthogonal states are noncommuting observables, the population of such states obeys uncertainty relations. It is in this context particularly relevant to consider the so-called mutually unbiased bases (MUBs) [3–6], which are defined by the property that the squared overlaps between a basis state in one basis and all basis states in the other bases are identical, and hence the detection of a particular basis state does not give away any information about the state if it was prepared in another basis. The original quantum cryptography protocol by Bennett and Brassard [7], with photons polarized along different sets of directions, and the later six-state protocol [8,9] exactly make use of the indistinguishability of states within MUBs.

In connection with information theory, the uncertainty relations may, as originally proposed by Deutsch [10], be reformulated in terms of entropies, and it is the purpose of the present article to derive uncertainty relations obeyed by entropies for mutually unbiased bases.

In Sec. II, we review some recently derived entropic uncertainty relations for mutually unbiased bases. In Sec. III, we present two mathematical results for the probabilities to measure certain basis vector states on a qudit (d-level) quantum system. In Sec. IV, we present a number of entropic uncertainty relations following from our mathematical results, and in Sec. V we conclude with a brief outlook.

II. MUTUALLY UNBIASED BASES AND ENTROPIC UNCERTAINTY RELATIONS

In a Hilbert space of finite dimension d, it is possible to identify mutually unbiased bases, but except for special cases, it is currently not known how many such bases exist. If d is a power of a prime $d=p^k$, there exist $d+1$ mutually unbiased bases, as exemplified by the three bases corresponding to the three orthogonal coordinate axes in the Bloch sphere representation of the qubit. For higher values of d it is only generally known that at last three mutually unbiased bases can always be identified, and it is a topic of ongoing research to search for more bases in, e.g., the lowest dimension, $d=6$, which is not a power of a prime [11].

In this section we will briefly summarize the results known about entropic uncertainty relations for MUBs.

For two incompatible observables, defined to have eigenstates which constitute a pair of MUBs, an entropic uncertainty relation was conjectured by Kraus [12] and was soon thereafter proved by Maassen and Uffink [13]. This relation can be expressed as follows:

$$H\{p_{i_1};i\}+H\{p_{i_2};i\}\geqslant \log_2 d, \tag{1}$$

where d is the dimension of the system and the Shannon entropy $H\{p_{i_m};i\}\equiv\sum_{i=1}^{d}-p_{i_m}\log_2 p_{i_m}$, with $p_{i_m}=\langle i_m|\rho|i_m\rangle$ being the probability of obtaining the ith result when the state ρ of a d-dimensional system is projected onto the mth basis $(m=1,2)$. Equation (1) constitutes an *information exclusion principle* with application in quantum communication, which may be readily adapted to take into account inexact measurements and added noise [14,15].

If we assume the existence of M MUBs, we can show that

$$\sum_{m=1}^{M} H\{p_{i_m};i\}\geqslant \frac{M}{2}\log_2 d. \tag{2}$$

If M is even, the result follows from (1) by grouping the MUBs in pairs. If M is odd, we can write the contribution from all basis states twice and make a new grouping of all bases and use (1) on the resulting pairs of different MUBs.

If the Hilbert space dimension is a square $d=r^2$, Ballester and Wehner [16] have shown that inequality (2) is tight when M does not exceed the maximal number of MUBs that exist for an r-dimensional system. By tight it is meant that a quantum state exists and is explicitly given by Ballester and Wehner, in which the equality sign holds in (2).

When the dimension of the system d is a power of a prime, $d+1$ MUBs exist and the entropic uncertainty relation for all MUBs,

$$\sum_{m=1}^{d+1} H\{p_{i_m};i\} \geqslant \begin{cases} (d+1)\log_2\left(\dfrac{d+1}{2}\right) & \text{when } d \text{ is odd},\\ \dfrac{d}{2}\log_2\left(\dfrac{d}{2}\right)+\left(\dfrac{d}{2}+1\right)\log_2\left(\dfrac{d}{2}+1\right) & \text{when } d \text{ is even},\end{cases} \tag{3}$$

was obtained by Ivanović [17] and Sanchez-Ruiz [18,19].

We shall now proceed to confirm, generalize, and extend the domain of validity of some of the results summarized above.

III. TWO NEW INEQUALITIES

The derivation of the best entropic uncertainty relation (3) for $d+1$ MUBs when d is a power of a prime is based on the equality $\sum_{m=1}^{d+1}\sum_{i=1}^{d}p_{i_m}^2=\mathrm{Tr}(\rho^2)+1$, which was obtained by Larsen [20] and Ivanović [17]; here, $p_{i_m}=\langle i_m|\rho|i_m\rangle$ denotes the probability of obtaining the ith result when projecting the state onto the mth MUB.

We shall first extend this equality to an inequality valid in the case of a number M of MUBs on a Hilbert space of arbitrary dimension.

Theorem 1. Suppose ρ is the state of a d-dimensional qudit, and let $p_{i_m}=\langle i_m|\rho|i_m\rangle$ denote the probability of obtaining the ith result when projecting the state onto the mth MUB. If M such MUBs exist, we have

$$\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2\leqslant \mathrm{Tr}(\rho^2)+\frac{M-1}{d}. \tag{4}$$

Proof. For the sake of the proof, consider two qudits a and b and a basis of the composite system ab that contains the following $M(d-1)+1$ orthonormal basis states:

$$|\Phi\rangle_{ab}=\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i_1\rangle_a\otimes|i_1\rangle_b^*, \tag{5}$$

$$|\phi_{m,k}\rangle_{ab}=\frac{1}{\sqrt{d}}\sum_{i=1}^{d}\omega^{k(i-1)}|i_m\rangle_a\otimes|i_m\rangle_b^*,$$

with $\omega=e^{2\pi i/d}$, $k=1,\ldots,d-1$, and $m=1,2,\ldots,M$ and with the remaining basis states denoted as $|\alpha_l\rangle_{ab}$ $[l=1,2,\ldots,L=d^2-M(d-1)-1]$. Here $|i_m\rangle^*$ denotes the "time-reversed" state of $|i_m\rangle$; i.e., for a definite basis—say, the first one $\{|i_1\rangle\}$—the basis vectors coincide, $|i_1\rangle=|i_1\rangle^*$, while all other bases differ by a complex conjugation of their expansion coefficients on the first basis.

Given any density matrix ρ of our single qudit, we define a two-qudit pure state $\rho_a\otimes I_b|\Phi\rangle_{ab}$ and expand it under the basis defined above:

$$\rho_a\otimes I_b|\Phi\rangle_{ab}=\frac{1}{d}|\Phi\rangle_{ab}+\sum_{m=1}^{M}\sum_{k=1}^{d-1}\rho_{mk}|\phi_{m,k}\rangle_{ab}+\sum_{l=1}^{L}c_l|\alpha_l\rangle_{ab}, \tag{6}$$

where $\rho_{mk}=\frac{1}{d}\sum_{i=1}^{d}\omega^{-k(i-1)}p_{i_m}$ with $p_{i_m}=\langle i_m|\rho|i_m\rangle$. A straightforward calculation yields

$$\begin{aligned}\sum_{m=1}^{M}\sum_{k=1}^{d-1}|\rho_{mk}|^2&=\frac{1}{d^2}\sum_{m=1}^{M}\sum_{k=1}^{d-1}\sum_{i,j=1}^{d}\omega^{-k(j-i)}p_{i_m}p_{j_m}\\&=\frac{1}{d^2}\sum_{m=1}^{M}\sum_{i,j=1}^{d}(d\delta_{ij}-1)p_{i_m}p_{j_m}\\&=\frac{1}{d}\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2-\frac{M}{d^2}.\end{aligned} \tag{7}$$

Thus

$$\begin{aligned}{}_{ab}\langle\Phi|\rho^2\otimes I|\Phi\rangle_{ab}=\frac{1}{d}\mathrm{Tr}(\rho^2)&\geqslant\frac{1}{d^2}+\sum_{m=1}^{M}\sum_{k=1}^{d-1}|\rho_{mk}|^2\\&=\frac{1}{d}\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2-\frac{M-1}{d^2},\end{aligned} \tag{8}$$

i.e.,

$$\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2\leqslant \mathrm{Tr}(\rho^2)+\frac{M-1}{d}. \tag{9}$$

This completes the proof.

Note that our construction of the two-qudit states resembles the Jamiolkowski isomorphism [21], and the expansion of $(\rho\otimes I)|\Phi\rangle_{ab}$ in (6) can indeed be viewed as an expansion of the operator ρ in terms of a set of orthonormal unitary operators in the Hilbert-Schmidt space of operators, including $\{I,\ U_{m,k}=\sum_{i=1}^{d}\omega^{k(i-1)}|i_m\rangle\langle i_m||k=1,\ldots,d-1,$ and $m=1,\ldots,M\}$.

Theorem 2. Following the same notation as above, we have the following entropic uncertainty relation for M MUBs of a qudit system in the state ρ,

$$\sum_{m=1}^{M} H\{p_{i_m};i\} \geq aC(K+1)\log_2(K+1) + (1-a)CK\log_2 K, \tag{10}$$

where $K=\lfloor\frac{M}{C}\rfloor$, $a=\frac{M}{C}-K$, and C has to be an upper bound for $\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2$. We can, for example, use (4) to choose $C=\mathrm{Tr}(\rho^2)+\frac{M-1}{d}$.

Proof. Our proof uses a result by Harremoës and Topsøe [22], which is conveniently formulated as the following.

Harremoës-Topsøe theorem. For any given probability distribution $\mathbf{p}=(p_1,p_2,\ldots,p_d)$, the Shannon entropy $H\{p_i;i\}$ and the so-called index of coincidence, $C\{p_i;i\}=\sum_i p_i^2$, obey the following inequality for arbitrary values of the integer $1\leq k\leq d-1$:

$$\begin{aligned} H\{p_i;i\} \geq{}& [(k+1)\log_2(k+1) - k\log_2 k] \\ &- k(k+1)[\log_2(k+1)-\log_2 k]C\{p_i;i\}. \end{aligned} \tag{11}$$

As a result

$$\begin{aligned} \sum_{m=1}^{M} H\{p_{i_m};i\} \geq{}& M[(k+1)\log_2(k+1) - k\log_2 k] \\ &- k(k+1)[\log_2(k+1)-\log_2 k]\sum_{m=1}^{M} C\{p_{i_m};i\}, \end{aligned} \tag{12}$$

Since $\sum_{m=1}^{M}C\{p_{i_m};i\}\leq C$, the upper bound for $\sum_{m=1}^{M}\sum_{i=1}^{d}p_{i_m}^2$, we immediately get

$$\begin{aligned} \sum_{m=1}^{M} H\{p_{i_m};i\} \geq{}& M[(k+1)\log_2(k+1) - k\log_2 k] - k(k+1) \\ &\times[\log_2(k+1)-\log_2 k]C \\ ={}& (M-kC)(k+1)\log_2(k+1) \\ &- [M-(k+1)C]k\log_2 k \end{aligned} \tag{13}$$

for any integer k with $1\leq k\leq d-1$.

The right-hand side of the above inequality can be viewed as a function of the integer k, which reaches its maximal value at $k=\lfloor M/C\rfloor$ when M/C is not an integer and which reaches the maximal value at both $k=\lfloor M/C\rfloor$ and $k=\lfloor M/C\rfloor-1$ when M/C is an integer (see the Appendix). Therefore, if we let $k=K=\lfloor M/C\rfloor$, we immediately get (10), which is the strongest inequality we can get from (13). This completes the proof of Theorem 2.

IV. ENTROPIC UNCERTAINTY RELATIONS

The uncertainty relations, cited in Sec. II, were all valid independently of the state occupied by the physical system. Using our propositions, we can derive state-dependent uncertainty relations, which must be obeyed for any MUBs for a given state ρ, and we can use our results to derive also general state independent uncertainty relations.

Proposition 3. For M MUBs of a qudit prepared in the state ρ, we have the following simple state-dependent entropic uncertainty inequality:

$$\sum_{m=1}^{M} H\{p_{i_m};i\} \geq M\log_2\frac{M}{C}, \tag{14}$$

with $C=\mathrm{Tr}(\rho^2)+\frac{M-1}{d}$. Using that $\mathrm{Tr}(\rho^2)\leq 1$, we obtain from (14) the following state-independent entropic uncertainty inequality:

$$\sum_{m=1}^{M} H\{p_{i_m};i\} \geq M\log_2\frac{Md}{d+M-1}. \tag{15}$$

Proof. By denoting the right-hand side of (10) as $f(K)$, from the convexity of the function $x\log_2 x$ we immediately have

$$\begin{aligned} f(K) &\geq C[a(K+1)+(1-a)K]\log_2[a(K+1)+(1-a)K] \\ &= M\log_2\frac{M}{C}, \end{aligned} \tag{16}$$

which implies (14). Furthermore, (15) follows from (14) since $\mathrm{Tr}(\rho^2)\leq 1$. Relation (14) also follows directly from (4) by the convexity of the function $-\log_2 x$.

When the number of MUBs is large compared with $\sqrt{d}+1$, or more precisely, when $M>[\mathrm{Tr}(\rho^2)-\frac{1}{d}]\frac{d}{\sqrt{d}-1}$, our relation (14) is stronger than (2). Also, when M is small compared with $\sqrt{d}+1$, relation (14) provides a stronger relation than (2) when the state ρ is sufficiently mixed.

Going back to the inequality (10) and making use of $\mathrm{Tr}(\rho^2)\leq 1$ to choose $C=1+\frac{M-1}{d}$ here, we get a state-independent inequality which is in fact stronger than (15) as follows.

Proposition 4.

$$\begin{aligned} \sum_{m=1}^{M} H\{p_{i_m};i\} \geq{}& [a(K+1)\log_2(K+1) \\ &+ (1-a)K\log_2 K]\frac{d+M-1}{d}, \end{aligned} \tag{17}$$

with $K=\lfloor\frac{Md}{d+M-1}\rfloor$ and $a=\frac{Md}{d+M-1}-K$. Inequality (17) can also be rewritten as

$$\sum_{m=1}^{M} H\{p_{i_m};i\} \geq M \log_2 K + (K+1) \times \left(M - K\frac{d+M-1}{d}\right)\log_2\left(1+\frac{1}{K}\right), \tag{18}$$

which is dominated by the first term when M is much larger than unity.

As any system with $d \geq 2$ has at least three MUBs, we will consider that case as an example, and note from (17) that

$$\sum_{m=1}^{3} H\{p_{i_m};i\} \geq \begin{cases} 2 & \text{for } d=2, \\ \frac{8}{3} & \text{for } d=3, \\ 3\left(1-\frac{4}{d}\right)\log_2 3 + \frac{12}{d} & \text{for } d \geq 4. \end{cases} \tag{19}$$

Unlike the restrictions on previously derived inequalities, the entropic uncertainty inequalities, derived here, work for any dimension d of the system and any number M of MUBs (assuming they exist). When d is a power of a prime, we know that there exist $d+1$ MUBs, and choosing $M=d+1$ in (17), we obtain the result in [19]:

$$\sum_{m=1}^{d+1} H\{p_{i_m};i\} \geq \begin{cases} (d+1)\log_2\left(\frac{d+1}{2}\right) & \text{when } d \text{ is odd}, \\ \frac{d}{2}\log_2\left(\frac{d}{2}\right) + \left(\frac{d}{2}+1\right)\log_2\left(\frac{d}{2}+1\right) & \text{when } d \text{ is even}. \end{cases} \tag{20}$$

Unlike the proof in [19], which works only when d is a power of a prime and $M=d+1$, our result (17) works for any d and any allowed number of MUBs M.

The state-dependent inequality with $C=\mathrm{Tr}(\rho^2)+\frac{M-1}{d}$ in (10) provides stronger bounds than (14) and (17). Consider, for example, the qubit case $d=2$, and suppose $M=3$, with $C=\mathrm{Tr}(\rho^2)+1$; from (10), we have

$$\sum_{m=1}^{3} H\{p_{i_m};i\} \geq 4 - 2\,\mathrm{Tr}(\rho^2). \tag{21}$$

This entropic uncertainty relation (21) is stronger than the result $\sum_{m=1}^{3} H\{p_{i_m};i\} \geq 2$ in [18,19], and it is also stronger than $\sum_{m=1}^{3} H\{p_{i_m};i\} \geq 3\log_2 \frac{3}{1+\mathrm{Tr}(\rho^2)}$ that follows from (14).

Remark. Inequality (4) itself can be viewed as an entropic uncertainty relation in terms of the Tsallis entropy, which is defined as $S_q^T\{p_i;i\} \equiv (1-\Sigma_i p_i^q)/(q-1)$ $(q>1)$ [23], with $q=2$ for our case. Similarly we can obtain inequalities obeyed by the $q=2$ Rényi entropy, defined by $S_q^R\{p_i;i\} \equiv \log_2(\Sigma_i p_i^q)/(1-q)$ $(q>1)$ [24]. Using the concavity property of the Rényi entropy and setting $q=2$, we get from (4) the inequality

$$\sum_{m=1}^{M} S_2^R\{p_{i_m};i\} \geq -M \log_2\left[\frac{1}{M}\left(\mathrm{Tr}\,\rho^2 + \frac{M-1}{d}\right)\right] \geq M \log_2 \frac{Md}{d+M-1}. \tag{22}$$

Let us finally consider the application of entropic uncertainty to composite systems. Let A and B denote subsystems with Hilbert space dimensions d_A and d_B, and let $\{|i_{mA}\rangle | i=1,\ldots,d_A\}$ and $\{|s_{nB}\rangle | s=1,\ldots,d_B\}$ denote the mth and nth mutually unbiased bases of systems A and B. We now consider local measurements on a bipartite state ρ_{AB} of the joint system. When system A is projected onto the mth MUB and system B is projected onto the nth MUB, the joint probability of outcomes in these bases is denoted by $p_{is}^{(m,n)} = \langle i_{mA}|\langle s_{nB}|\rho_{AB}|i_{mA}\rangle|s_{nB}\rangle$. The entropic uncertainty inequalities we have derived above can now be applied to the composite system, and in particular we can derive the following.

If ρ_{AB} is a separable state, then for M MUBs of each subsystem we have

$$\sum_{m=1}^{M} H\{p_{is}^{(m,m)};is\} \geq M \log_2 K_A + (K_A+1)\left(M - K_A\frac{d_A+M-1}{d_A}\right)\log_2 \times \left(1+\frac{1}{K_A}\right) + M\log_2 K_B + (K_B+1) \times \left(M - K_B\frac{d_B+M-1}{d_B}\right)\log_2\left(1+\frac{1}{K_B}\right), \tag{23}$$

with $K_{A(B)} = \lfloor \frac{M d_{A(B)}}{d_{A(B)}+M-1} \rfloor$.

Proof. If ρ_{AB} is separable, it can be written as a convex sum of product states: $\rho_{AB} = \Sigma_j q_j \rho_j^A \otimes \rho_j^B$. Therefore we have

$$\sum_{m=1}^{M} H\{p_{is}^{(m,m)};is\}_\rho \geq \sum_j q_j \sum_{m=1}^{M} H\{p_{is}^{(m,m)};is\}_{\rho_j^A\otimes\rho_j^B} = \sum_j q_j \sum_{m=1}^{M} H\{p_i^{(m)};i\}_{\rho_j^A} + \sum_j q_j \sum_{m=1}^{M} H\{p_s^{(m)};s\}_{\rho_j^B}. \tag{24}$$

The proposition immediately follows from the above inequality and (18).

As an example, when $d_A=d_B=2$ and $M=3$, for a separable state ρ_{AB} we have

$$\sum_{m=1}^{3} H\{p_{is}^{(m,m)};is\} \geq 4. \tag{25}$$

It should be noted that this separability criterion is not a strong one, and replacing the inequality sign by an equality it does not even for qubits provide the actual boundary between separable and entangled states. The result, however, is an example of how the concavity of entropy functions together with entropic uncertainty relations can provide insights into the topic of entanglement.

V. CONCLUSION

In this paper we have presented a number of inequalities obeyed by the probability distributions for measurements on quantum systems in mutually unbiased bases. We have obtained tighter and more general entropic uncertainty relations than the ones presented in the literature, and we have given less tight, but more compact, expressions in simple cases. In the Introduction we motivated the work by the application of complementarity and uncertainty relations in quantum information theory. Entropy is used to quantify information, and hence entropic uncertainty relations provide bounds on the information obtainable by measurements of different observables of a quantum system. The more general inequalities derived and proven in this article thus form the basis for more quantitative results on this topic.

ACKNOWLEDGMENTS

The authors wish to thank Uffe V. Poulsen and the MOBISEQ network under the Danish Natural Science Research Council for helpful discussions. S.W. and S.Y. also wish to acknowledge support from the NNSF of China (Grants No. 10604051 and No. 10675107), the CAS, and the National Fundamental Research Program.

APPENDIX

Denoting

$$f(x) = (M - Cx)(x+1)\ln(x+1) - [M - C(x+1)]x \ln x$$

and $K=\lfloor \frac{M}{C} \rfloor$, we shall prove $\max_k f(k) \leqslant f(K)$. Here k is any integer and $1 \leqslant k \leqslant d-1$. $g(x)= x\ln x-(1+x)\ln(1+x)$ is a decreasing function of $x \geqslant 0$ since $g'(x)=\ln \frac{x}{1+x} < 0$. Thus $g(k+1) < g(k)$—i.e.,

$$2\ln(k+1)^{k+1} - \ln k^k (k+2)^{k+2} < 0.$$

Denote $\Delta(x)=f(x)-f(x+1)$, which reads

$$\Delta(k) = [M - C(k+1)][2\ln(k+1)^{k+1} - \ln k^k (k+2)^{k+2}].$$

If $\lfloor \frac{M}{C} \rfloor$ is not an integer, then $\frac{M}{C}-1 < K < \frac{M}{C}$ and $\Delta(K-1) < 0$, so $f(K-1) < f(K)$, and $\Delta(K) > 0$, so $f(K) > f(K+1)$. So the maximal value of $f(k)$ over integer k is obtained at $k=K$. If $\lfloor \frac{M}{C} \rfloor$ is an integer, then $K=\frac{M}{C}$ and $\Delta(K-1)=0$, so $f(K-1)=f(K)$; similarly, we can show $f(K-2) < f(K-1)$ and $f(K+1) < f(K)$. So the maximal value of $f(k)$ over integer k is obtained at both $k=K$ and $k=K-1$. Therefore $\max_k f(k) \leqslant f(K)$.

[1] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[2] E. Schrödinger, Sitzungsber. Preuss. Akad. Wiss., Phys. Math. Kl. **19**, 296 (1930).
[3] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).
[4] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[5] A. Klappenecker and M. Roetteler, e-print arXiv:quant-ph/0309120.
[6] A. O. Pittenger and M. H. Rubin, Linear Algebr. Appl. **390**, 255 (2004).
[7] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.
[8] D. Bruss, Phys. Rev. Lett. **81**, 3018–3021 (1998).
[9] H. Bechmann-Pasquinucci and N. Gisin, e-print arXiv:quant-ph/9807041.
[10] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[11] I. Bengtsson *et al.*, J. Math. Phys. **48**, 052106 (2007).
[12] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[13] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[14] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).
[15] M. J. W. Hall, Phys. Rev. A **55**, 100 (1997).
[16] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[17] I. D. Ivonovic, J. Phys. A **25**, L363 (1992).
[18] J. Sánchez, Phys. Lett. A **173**, 233 (1993).
[19] J. Sánchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[20] U. Larsen, J. Phys. A **23**, 1041 (1990).
[21] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[22] P. Harremoes and F. Topsoe, IEEE Trans. Inf. Theory **47**, 2944 (2001).
[23] C. Tsallis, J. Stat. Phys. **52**, 479 (1988).
[24] A. Rényi, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability*, edited by J. Neyman (University of California Press, Berkeley, 1961), Vol. 1, pp. 547–561.