Improved uncertainty relation in the presence of quantum memory

Yunlong Xiao¹,², Naihuan Jing³,⁴, Shao-Ming Fei²,⁵ and Xianqing Li-Jost²

¹ School of Mathematics, South China University of Technology, Guangzhou, Guangdong 510640, People’s Republic of China
² Max Planck Institute for Mathematics in the Sciences, 04103 Leipzig, Germany
³ Department of Mathematics, Shanghai University, Shanghai 200436, People’s Republic of China
⁴ Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA
⁵ School of Mathematical Sciences, Capital Normal University, Beijing 100048, People’s Republic of China

E-mail: jing@ncsu.edu

Received 25 June 2016, revised 25 October 2016
Accepted for publication 31 October 2016
Published 16 November 2016

Abstract
Berta et al.’s uncertainty principle in the presence of quantum memory (Berta et al 2010 Nat. Phys. 6 659) reveals uncertainties with quantum side information between the observables. In the recent important work of Coles and Piani (2014 Phys. Rev. A 89 022112), the entropic sum is controlled by the first and second maximum overlaps between the two projective measurements. We generalize the entropic uncertainty relation in the presence of quantum memory and find the exact dependence on all $d$ largest overlaps between two measurements on any $d$-dimensional Hilbert space. Our bound is rigorously shown to be strictly tighter than previous entropic bounds in the presence of quantum memory, which have potential applications to quantum cryptography with entanglement witnesses and quantum key distributions.

Keywords: uncertainty relations, entropy, quantum memory

(Some figures may appear in colour only in the online journal)
Heisenberg’s uncertainty principle [1] plays a central role in physics and marks a distinguished characteristic of quantum mechanics. The principle bounds the uncertainties of measurement outcomes of two observables, such as the position and momentum of a particle. This shows the underlying difference of quantum mechanics from classical mechanics where any properties of a physical object can be quantified exactly at the same time. In Robertson’s formulation [2], the product of the standard deviations (denoted by $\Delta(R)$ for the observable $R$) of the measurement of two observables $R$ and $S$ is controlled by their commutator:

$$\Delta R \Delta S \geq \frac{1}{2} |\langle [R, S] \rangle|,$$

(1)

where $\langle \cdot | \cdot \rangle$ is the expectation value. The relation implies that it is impossible to simultaneously measure exactly a pair of incompatible (noncommutative) observables.

In the context of both classical and quantum information sciences, it is more natural to use entropy to quantify uncertainties [3, 4]. The first entropic uncertainty relation for position and momentum was given in [5] (which can be shown to be equivalent to Heisenberg’s original relation). Later Deutsch [6] found an entropic uncertainty relation for any pair of observables. An improvement of Deutsch’s entropic uncertainty relation was subsequently conjectured by Kraus [7] and later proved by Maassen and Uffink [8] (we use base 2 log throughout this paper),

$$H(R) + H(S) \geq \log \frac{1}{c_1},$$

(2)

where $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ are two orthonormal bases on $d$-dimensional Hilbert space $\mathcal{H}_A$, and $H(R) = -\sum_i p_i \log p_i$ is the Shannon entropy of the probability distribution $\{p_j = \langle u_j | \rho_A | u_j \rangle\}$ for state $\rho_A$ (similarly for $H(S)$ and $\{q_k = \langle v_k | \rho_A | v_k \rangle\}$). The number $c_1$ is the largest overlap among all $c_{jk} = |\langle u_j | v_k \rangle|^2$ ($\leq 1$) between the projective measurements $R$ and $S$.

One of the important recent advances on uncertainty relations is to allow the measured quantum system to be correlated with its environment in a non-classical way, for instance, picking up quantum correlations such as entanglement in quantum cryptography. Historically, the entropic uncertainty relations have inspired initial formulation of quantum cryptography. But the uncertainty relations in the absence of quantum memory did not leave any chance for an eavesdropper to have access to the quantum correlations. Therefore the ‘classical’ uncertainty relations without quantum side information cannot be utilized to improve cryptographic security directly. Berta et al [9] bridged the gap between cryptographic scenarios and the uncertainty principle, and derived this landmark uncertainty relation for measurements $R$ and $S$ in the presence of quantum memory $B$:

$$H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + H(A|B),$$

(3)

where $H(R|B) = H(\rho_{RB}) - H(\rho_B)$ is the conditional entropy with $\rho_{RB} = \sum_j |u_j\rangle \langle u_j| \otimes I(\rho_A)(|u_j\rangle \langle u_j| \otimes I)$ (similarly for $H(S|B)$), and $d$ is the dimension of the subsystem $A$. The term $H(A|B) = H(\rho_A) - H(\rho_B)$ appearing on the right-hand side is related to the entanglement between the measured particle $A$ and the quantum memory $B$.

The bound of Berta et al has recently been upgraded by Coles and Piani [10], who have shown a remarkable bound in the presence of quantum memory.
\[ H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + H(A|B), \tag{4} \]

where \( c_2 \) is the second largest overlap among all \( c_{jk} \) (counting multiplicity) and other notations are the same as in equation (2). As \( 1 \geq c_1 \geq c_2 \), the second term in equation (4) shows that the uncertainties depend on more detailed information of the transition matrix or overlaps between the two bases. The Coles–Piani bound offers a strictly tighter bound than the bound of Berta et al as long as \( 1 > c_1 > c_2 \). The goal of this paper is to report a more general and tighter bound for the entropic uncertainty relation with quantum side information.

As reported in [11], there are some examples where the bounds such as \( B_{MG} \) and \( B_{RPZ} \) based on majorization approach outperform the degenerate form of Coles and Piani’s new bound in the special case when quantum memory is absent. However, it is unknown if these bounds and their approaches can be extended to allow for quantum side information (see [4]). Therefore Coles and Piani’s remarkable bound equation (4) is still the strongest lower bound for the entropic sum in the presence of quantum memory \textit{up to now}. In this paper, we improve the bound of Coles and Piani in the most general situation with quantum memory. Moreover, our new general bound is proven stronger by rigorous mathematical arguments.

To state our result, we first recall the majorization relation between two probability distributions \( P = (p_1, \ldots, p_d) \) and \( Q = (q_1, \ldots, q_d) \). The partial order \( P \prec Q \) means that \( \sum_{j=1}^i p_j \leq \sum_{j=1}^i q_j \) for all \( i = 1, \ldots, d \). Here \( ^1 \) denotes rearranging the components of \( p \) or \( q \) in descending order. Any probability distribution vector \( P \) is bounded by \( (\frac{d}{\sqrt{d}}, \ldots, \frac{1}{\sqrt{d}}) \prec (1, 0, \ldots, 0) = \{1\} \).

For any two probability distributions \( P = (p_i) \) and \( Q = (q_i) \) corresponding to measurements \( R \) and \( S \) of the state \( \rho \), there is a state-independent bound of direct-sum majorization [11]: \( P \oplus Q \prec \{1\} \oplus W \), where \( P \oplus Q = (p_1, \ldots, p_d, q_1, \ldots, q_d) \) and \( W = (s_1, s_2 - s_1, \ldots, s_d - s_{d-1}) \) is a special probability distribution vector defined exclusively by the overlap matrix related to \( R \) and \( S \). Let \( U = ((u_j|v_k))_{jk} \) be the overlap matrix between the two bases given by \( R \) and \( S \), and define the subset \( \text{Sub}(U, k) \) to be the collection of all size \( r \times s \) submatrices \( M \) such that \( r + s = k + 1 \). Following [11, 12] we define \( s_i = \max\{||M||: M \in \text{Sub}(U, k)\} \), where \( ||M|| \) is the maximal singular value of \( M \). Denote the sum of the largest \( k \) terms in \( \{1\} \oplus W \) as \( \Omega_k = 1 + s_{k-1} \) and the \( i \)-th largest overlap among \( c_{jk} \)’s as \( c_i \). Meanwhile \( s_0 = 0, s_1 = \sqrt{c_1} \) and \( s_d = 1 \). If follows from the basic definitions of \( \Omega_k \) that the following inequalities hold

\[ 1 = \Omega_1 \leq \Omega_2 \leq \cdots \leq \Omega_{d+1} = \cdots = \Omega_{2d} = 2, \]

where we noted that \( \Omega_2 = 1 + \sqrt{c_1} \).

Our main result is the following entropic uncertainty relation that, much like Coles–Piani’s bound, accounts for the possible use of a quantum side information due to the entanglement between the measured particle and quantum memory. For a bipartite quantum state \( \rho_{AB} \) on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \), we still use \( H \) to denote the von Neumann entropy, \( H(\rho_{AB}) = -\text{Tr}(\rho_{AB} \log \rho_{AB}) \).

**Theorem.** Let \( R = \{|u_i\rangle\} \) and \( S = \{|v_k\rangle\} \) be arbitrary orthonormal bases of the \( d \)-dimensional subsystem \( A \) of a bipartite state \( \rho_{AB} \). Then we have that

\[
H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + \frac{2 - \Omega_4}{2} \log \frac{c_2}{c_3} + \cdots + \frac{2 - \Omega_{2(d-1)}}{2} \log \frac{c_{d-1}}{c_d} + H(A|B), \tag{5}
\]
where \( H(R|B) = H(\rho_{RB}) - H(\rho_B) \) is the conditional entropy with \( \rho_{RB} = \sum_i \langle u_i | \langle u_i | \otimes I(\rho_{AB}) \rangle \langle u_i | \otimes I \rangle \) (similarly for \( H(S|B) \)), and \( H(A|B) = H(\rho_{AB}) - H(\rho_B) \).

We remark that due to \( \Omega_{d+1} = \cdots = \Omega_{2d} = 2 \), the last (non-zero) term of formula (17) can be fine-tuned according to the parity of \( d \). If \( d = 2n \), it is \( \log c_{2n} c_{2n}^2 \) for every \( j \); if \( d = 2n + 1 \), it is \( \log c_{2n+1} c_{2n+1}^2 \).

**Proof.** For completeness we start from the derivation of the Coles–Piani inequality. Observe that the quantum channel \( \rho \rightarrow \rho_{SB} \) is in fact \( \sum_k |v_k \rangle \langle v_k | \otimes \text{Tr}_d(\langle |v_k \rangle \langle v_k | \otimes I) \rho_{AB} \rangle \).

As the relative entropy \( D(\rho(\sigma) = \text{Tr}(\rho \log \rho) - \text{Tr}(\rho \log \sigma) \) is monotonic under a quantum channel it follows that

\[
H(S|B) - H(A|B) = D(\rho_{SB}) \sum_k \langle v_k | \langle v_k | \otimes I \rangle \rho_{AB} \rangle \langle v_k | \otimes I \rangle
\]

\[
\geq D(\rho_{RB}) \sum_k c_k |u_k \rangle \langle u_k | \otimes \text{Tr}_d(\langle |v_k \rangle \langle v_k | \otimes I) \rho_{AB} \rangle
\]

\[
= -H(R|B) - \sum_j p_j \log \max_k c_{jk},
\]

where the first expression of equation (6) is a basic identity of the quantum relative entropy (see [13, 14]). So the state-dependent bound under a quantum memory follows:

\[
H(R|B) + H(S|B) \geq H(A|B) - \sum_j p_j \log \max_k c_{jk}.
\]

Interchanging \( R \) and \( S \) we also have

\[
H(R|B) + H(S|B) \geq H(A|B) - \sum_k q_k \log \max_j c_{jk}.
\]

We arrange the numbers \( \max_k c_{jk}, j = 1, \ldots, d \), in descending order:

\[
\max_k c_{jk} \geq \max_k c_{j,k} \geq \cdots \geq \max_k c_{i,k}.
\]

where \( j_1 j_2 \cdots j_k \) is a permutation of \( 1 \cdots d \). Clearly \( c_1 = \max_k c_{j,k} \) and in general \( c_i \geq \max_k c_{j,k} \) for all \( i \). Therefore

\[
-\sum_{j=1}^d p_j \log \max_k c_{jk} = -\sum_{j=1}^d p_j \log \max_k c_{j,k} \geq -p_1 \log c_1 - p_2 \log c_2 - \cdots - p_d \log c_d
\]

\[
= -(1 - p_1 \cdots - p_d) \log c_1 - p_2 \log c_2 - \cdots - p_d \log c_d
\]

\[
= -\log c_1 + p_2 \log \frac{c_1}{c_2} + \cdots + p_d \log \frac{c_1}{c_d}.
\]

Similarly we also have

\[
-\sum_k q_k \log \max_j c_{jk} \geq -\log c_1 + q_2 \log \frac{c_1}{c_2} + \cdots + q_d \log \frac{c_1}{c_d}.
\]
for some permutation $k_1 k_2 \cdots k_d$ of $12 \cdots d$. Taking the average of equations (7) and (8) and plugging in equations (10) and (11) we have that

$$H(R|B) + H(S|B) \geq H(A|B) + \log \frac{1}{c_1} + \frac{p_h + q_{k_1}}{2} \log \frac{c_1}{c_2} + \cdots + \frac{p_{k_d} + q_d}{2} \log \frac{c_1}{c_d}.$$ (12)

Using $p_{k_i} + q_{k_i} = \sum_{j=1}^{d} (p_h + q_{k_i}) - \sum_{i=1}^{d} (p_h + q_{k_i})$ we see that equation (12) can be written equivalently as

$$H(R|B) + H(S|B) \geq H(A|B) + \log \frac{1}{c_1} + \frac{1}{2} \sum_{i=2}^{d} (p_h + q_{k_i}) \log \frac{c_i}{c_2} + \cdots + \frac{p_{k_d} + q_d}{2} \log \frac{c_i}{c_d}.$$ (13)

The above transformation from equation (12) to equation (13) adds all later coefficients of $\log \frac{c_2}{c_1}, \ldots, \log \frac{c_d}{c_1}$ into that of $\log \frac{c_2}{c_1}$ and modify the argument of each log to $\log \frac{c_2}{c_1}, \ldots, \log \frac{c_d}{c_1}$. Continuing in this way, we can write equation (13) equivalently as

$$H(R|B) + H(S|B) = H(A|B) - \log c_1 + \frac{2 - (p_h + q_{k_1})}{2} \log \frac{c_1}{c_2} + \frac{2 - \sum_{i=2}^{d-1} (p_h + q_{k_i})}{2} \log \frac{c_{d-1}}{c_d}.$$ (14)

Since $P \oplus Q \prec \{1\} \oplus W$, we have $p_h + q_{k_1} \leq \Omega_{2d-1}$, $p_h + q_{k_1} \leq \Omega_{2d-1}$, $p_h + q_{k_1} \leq \Omega_{2d-1}$. Plugging these into equation (12) completes the proof.

We remark that our newly constructed bound is stronger than Coles–Piani’s bound in all cases except when the observables are mutually unbiased (i.e. $c_{d-1} = |\langle u_j | u_k \rangle|^2 = 1/d$ for any $j, k$).

As an example, consider the following $2 \times 4$ bipartite state,

$$\rho_{AB} = \frac{1}{1 + 7p} \begin{pmatrix}
    p & 0 & 0 & 0 & 0 & p & 0 & 0 \\
    0 & p & 0 & 0 & 0 & 0 & p & 0 \\
    0 & 0 & p & 0 & 0 & 0 & p & 0 \\
    0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & \frac{1 + p}{2} & 0 & 0 & \frac{\sqrt{1 - p^2}}{2} \\
    0 & 0 & 0 & 0 & 0 & p & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & p & 0 \\
    0 & 0 & 0 & 0 & \frac{\sqrt{1 - p^2}}{2} & 0 & 0 & \frac{1 + p}{2}
\end{pmatrix},$$ (15)

which is known to be entangled for $0 < p < 1$ [15]. We take system $A$ as the quantum memory, consider the following two projective measurements: $\{ |\psi_j \rangle \}$ are the standard orthonormal basis on $H_B$ and $\{ |u_j \rangle \}$ are given by
Then the overlap matrix $(|u_j u_k^T|)$ is given by

\[
\begin{pmatrix}
144 & 36 & 16 & 9 \\
205 & 205 & 205 & 205 \\
4356 & 29584 & 33489 & 104976 \\
172405 & 172405 & 172405 & 172405 \\
121 & 95481 & 76050 & 1458 \\
250618 & 250618 & 125309 & 125309 \\
81 & 81 & 18 & 50 \\
298 & 298 & 149 & 149
\end{pmatrix}.
\]  

(16)

Thus $\Omega_4 = 2$ and $c_2 = c_3$. The comparison between Coles–Piani’s bound and equation (5) in the presence of quantum memory is displayed in figure 1, which shows that our new bound is strictly tighter for all $p \in (0, 1)$.

After presenting the general result, we now turn to its special situation for the state-independent bound in the absence of quantum memory. As many state-independent bounds cannot be generalized to the general situation, a separate treatment is needed and one will see that our new bound fares reasonably well even in the absence of quantum memory.

**Corollary.** Let $R = \{|u_j\}$ and $S = \{|v_k\}$ be any two orthonormal bases on $d$-dimensional Hilbert space $\mathcal{H}_A$. Then for any state $\rho_A$ over $\mathcal{H}_A$, we have the following inequality:

\[
H(R) + H(S) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + \frac{2 - \Omega_4}{2} \log \frac{c_2}{c_3} + \cdots + \frac{2 - \Omega_{2(d-1)}}{2} \log \frac{c_{d-1}}{c_d},
\]

where $\Omega_k$ and $c_i$ are defined in equation (5).

The corollary can be similarly proved due to the following simple observation. When measurements are performed on system $A$, $H(R) + H(S) \geq -\sum_j p_j \log \sum_k q_k c_{jk} + H(A) \geq -\sum_j p_j \log \max_k c_{jk} + H(A)$. Then the corollary follows directly from the proof of the theorem.

We now compare our bound given in the corollary with some of the well-known bounds in this special case. First of all, our new bound is clearly tighter than Coles–Piani’s bound
as we have already shown mathematically. In [11] Rudnicki et al obtained the direct-sum majorization bound, one of the major ones for the state-independent states, thus we will focus on comparing our bound with this one. Consider the following unitary matrices between two measurements

\[ U(\theta) = M(\theta) OM(\theta)^\dagger, \tag{18} \]

where \( \theta \in [0, \pi/4] \) and

\[ M(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta_1 & \sin \theta_1 \\ 0 & -\sin \theta_1 & \cos \theta_1 \end{pmatrix}, \tag{19} \]

with the overlap matrix

\[ O = \begin{pmatrix} 0.4575 & 0.4575 & 0.7625 \\ -0.2453 & 0.8892 & -0.3863 \\ -0.8547 & -0.0103 & 0.5190 \end{pmatrix}. \tag{20} \]

Figure 2 shows that the direct-sum majorization bound and our bound equation (17) are complementary, as there are regions where our bound is tighter. This implies that our bound in this special case is also nontrivial. We would like to remark that there are other bounds for the entropic uncertainty relations in the absence of quantum side information, but most of them cannot be generalized to the case with quantum memory.

Note that the overlaps, which are commonly used in entropic uncertainty relations, are state-independent measurements so we can only consider them when the experimental device is trusted. For device-independent uncertainty based on state-dependent and incompatible measures, see [16]. There seems no clear relation between our bound and the bound based on state-dependent anticommutators, and it is still open whether the approach of [16] based on state-dependent measurements can be extended to allow for the quantum side information. On the other hand, our result holds for the general case with the quantum side information.
Conclusion

We have found new lower bounds for the sum of the entropic uncertainties in the presence of quantum memory. Our new bounds have formulated the complete dependence on all $d$ largest entries in the overlap matrix between two measurements on a $d$-dimensional Hilbert space, while the previously best-known bound involves with the first two largest entries. We have shown that our bounds are strictly tighter than previously known entropic uncertainty bounds with quantum side information by mathematical argument in the general situation. In the special case without quantum memory, our bound also offers significant new information as it is complementary to some of the best known bounds in this situation. Moreover, as entropic uncertainty relations in the presence of quantum memory have a wide range of applications, our results are expected to shed new lights on investigation of quantum information processing such as information exclusive relation [17], entanglement detection, quantum key distribution and other cryptographic scenarios.

Acknowledgments

The work is supported by NSFC (grant Nos. 11271138, 11531004, 11275131, 11675113), CSC and Simons Foundation grant 198129.

References

[1] Heisenberg W 1927 Z. Phys. 43 172
[2] Robertson H P 1929 Phys. Rev. 34 163
[3] Bialynicki-Birula I and Rudnicki L 2011 Statistical Complexity ed K Sen (Dordrecht: Springer) pp 1–34
[4] Coles P J, Berta M, Tomamichel M and Wehner S 2015 arXiv:1511.04857v1
[5] Bialynicki-Birula I and Mycielski J 1975 Commun. Math. Phys. 44 129
[6] Deutsch D 1983 Phys. Rev. Lett. 50 631
[7] Kraus K 1987 Phys. Rev. D 35 3070
[8] Maassen H and Uffink J B M 1988 Phys. Rev. Lett. 60 1103
[9] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 Nat. Phys. 6 659
[10] Coles P J and Piani M 2014 Phys. Rev. A 89 022112
[11] Rudnicki Ł, Puchała Z and Życzkowski K 2014 Phys. Rev. A 89 052115
[12] Puchała Z, Rudnicki Ł and Życzkowski K 2013 J. Phys. A: Math. Theor. 46 272002
[13] Coles P J, Yu L, Gheorghiu V and Griffiths R B 2011 Phys. Rev. A 83 062338
[14] Coles P J 2012 Phys. Rev. A 85 042103
[15] Bennett C H, DiVincenzo D P, Mor T, Shor P W, Smolin J A and Terhal B M 1999 Phys. Rev. Lett. 82 5385
[16] Kaniewski J, Tomamichel M and Wehner S 2014 Phys. Rev. A 90 012332
[17] Xiao Y, Jing N and Li-Jost X 2016 Sci. Rep. 6 30440