Extensions of the quantum Fano inequality

Naresh Sharma
Tata Institute of Fundamental Research
Mumbai 400 005, India
nsharma@tifr.res.in

October 26, 2018

Abstract

Quantum Fano inequality (QFI) in quantum information theory provides an upper bound to the entropy exchange by a function of the entanglement fidelity. We give various Fano-like upper bounds to the entropy exchange and QFI is a special case of these bounds. These bounds also give an alternate derivation of the QFI.

1 Introduction

Classical Fano inequality (CFI) in classical information theory provides an upper bound to the conditional entropy of two correlated random variables say $X$ and $Y$. Suppose we wish to obtain an estimate of $X$ when $Y$ is known. To get an estimate of $X$, we compute a function of $Y$, denoted by $\hat{X}$. Let $n$ be the cardinality of the set from which $X$ takes values. CFI upper bounds the conditional Shannon entropy of $X$ given $Y$, denoted by $H_S(X|Y)$, by a function of the probability of success defined as

$$P_s = \Pr\{\hat{X} = X\} \quad (1)$$

(see p. 37 in [1]) and is given by

$$H_S(X|Y) \leq H(P_s) + (1 - P_s) \ln(n - 1), \quad (2)$$

where

$$H(x) = -x \ln(x) - (1 - x) \ln(1 - x) \quad (3)$$

is the binary entropy function. CFI is useful in proving the converse to the Shannon’s noisy channel coding theorem (see p. 206 in Ref. [1]).

QFI provides an upper bound to the entropy exchange by a function of the entanglement fidelity, and the function is similar to the function of success used in the CFI.

More specifically, let $R$ and $Q$ be two quantum systems described by a Hilbert space $\mathcal{H}_Q$ of finite dimension $d$, where $d \geq 2$. The joint system $RQ$ is initially prepared in a pure entangled state

$$|\psi^{RQ}\rangle = \sum_{k=1}^{d} \sqrt{\lambda_k} |k^R\rangle |k^Q\rangle, \quad (4)$$
where $\lambda = [\lambda_1 \cdots \lambda_d]$ is a probability vector, i.e., $\lambda_k \geq 0$, $\sum_{k=1}^d \lambda_k = 1$, $\{|k^R\rangle\}$ and $\{|k^Q\rangle\}$, $k = 1, \ldots, d$, are two orthonormal bases for $\mathcal{H}_Q$. $|\psi^{RQ}\rangle$ is a purification of $\rho$, the state of system $Q$, and

$$\rho = \text{Tr}_R(|\psi^{RQ}\rangle\langle\psi^{RQ}|) = \sum_{k=1}^d \lambda_k |k^Q\rangle\langle k^Q|.$$  \hfill (5)

The system $Q$ undergoes a completely positive trace-preserving transformation or quantum operation $E$ and $R$ is assumed to be isolated and its state remains the same. This quantum operation is also represented by $I_R \otimes E$, where $I_R$ is the identity superoperator on $R$. We add subscript “1” to denote the state of the system (joint or otherwise) after this quantum operation. So the state of the joint system is denoted by $\rho_{R1Q1}$. Note that $\rho_{Q1} = E(\rho)$ and $\rho_{R1} = \rho_R$.

The entanglement fidelity is defined by Schumacher \cite{2} as

$$F(\rho, E) = \langle \psi^{RQ}| \rho_{R1Q1} | \psi^{RQ}\rangle$$  \hfill (6)

and the entropy exchange as

$$S(\rho, E) = S(\rho_{R1Q1}),$$  \hfill (7)

where $S(\rho_{R1Q1})$ is the von-Neumann entropy of $\rho_{R1Q1}$. The QFI upper bounds $S(\rho, E)$ by a function of the entanglement fidelity as \cite{2}

$$S(\rho, E) \leq H(F(\rho, E)) + (1 - F(\rho, E)) \ln (d^2 - 1).$$  \hfill (8)

More details on the QFI can be found in Ref. \cite{2}, p. 563 in Ref. \cite{3}, p. 222 in Ref. \cite{4}.

Generalization of the CFI was provided by Han and Verdú \cite{5}, where various lower bounds to the mutual information are given.

In this paper, we give extensions of the QFI and give various Fano-like upper bounds to $S(\rho, E)$. One of the bounds that we derive for any probability vector $\gamma = [\gamma_1 \cdots \gamma_d]$ is

$$S(\rho, E) \leq H(F(\rho, E)) + \ln \left( \sum_{i=1}^d \lambda_i \gamma_i \right) + (1 - F(\rho, E)) \ln \left( \frac{d}{\sum_{i=1}^d \lambda_i \gamma_i} - 1 \right) - \sum_{k=1}^d \lambda_k \ln(\gamma_k),$$  \hfill (9)

where using Eq. \cite{5}, $\lambda_i$, $i = 1, \ldots, d$, are the eigenvalues of $\rho$. It is easy to see that Eq. \cite{8} is a special case of Eq. \cite{9} by substituting $\gamma_i = 1/d$, $i = 1, \ldots, d$. Our approach also gives an alternate derivation of the QFI.

## 2 Extensions of the Quantum Fano inequality

Let $R_2$, $Q_2$ be two ancilla quantum systems, possibly entangled, described by $\mathcal{H}_Q$. The joint system $R_2Q_2$ is described by $\mathcal{H}_{RQ} = \mathcal{H}_Q \otimes \mathcal{H}_Q$, and let $\{|k^{RQ}\rangle\}$ be an orthonormal basis for $\mathcal{H}_{RQ}$, and we define a set of projectors as

$$P_k = |k^{RQ}\rangle\langle k^{RQ}|,$$  \hfill (10)

where we have chosen

$$|1^{RQ}\rangle = |\psi^{RQ}\rangle,$$  \hfill (11)

and the entropy exchange as

$$S(\rho, E) = S(\rho_{R1Q1}),$$  \hfill (7)

where $S(\rho_{R1Q1})$ is the von-Neumann entropy of $\rho_{R1Q1}$. The QFI upper bounds $S(\rho, E)$ by a function of the entanglement fidelity as \cite{2}

$$S(\rho, E) \leq H(F(\rho, E)) + (1 - F(\rho, E)) \ln (d^2 - 1).$$  \hfill (8)

More details on the QFI can be found in Ref. \cite{2}, p. 563 in Ref. \cite{3}, p. 222 in Ref. \cite{4}.

Generalization of the CFI was provided by Han and Verdú \cite{5}, where various lower bounds to the mutual information are given.

In this paper, we give extensions of the QFI and give various Fano-like upper bounds to $S(\rho, E)$. One of the bounds that we derive for any probability vector $\gamma = [\gamma_1 \cdots \gamma_d]$ is

$$S(\rho, E) \leq H(F(\rho, E)) + \ln \left( \sum_{i=1}^d \lambda_i \gamma_i \right) + (1 - F(\rho, E)) \ln \left( \frac{d}{\sum_{i=1}^d \lambda_i \gamma_i} - 1 \right) - \sum_{k=1}^d \lambda_k \ln(\gamma_k),$$  \hfill (9)

where using Eq. \cite{5}, $\lambda_i$, $i = 1, \ldots, d$, are the eigenvalues of $\rho$. It is easy to see that Eq. \cite{8} is a special case of Eq. \cite{9} by substituting $\gamma_i = 1/d$, $i = 1, \ldots, d$. Our approach also gives an alternate derivation of the QFI.
and \( I^{RQ} \) is the \( d^2 \times d^2 \) identity matrix. Then

\[
S(\rho, E) = S(\rho^{R_1Q_1})
= -S(\rho^{R_1Q_1}||\rho^{R_2Q_2}) - \text{Tr}(\rho^{R_1Q_1} \ln(\rho^{R_2Q_2}))
\leq -S \left( \sum_{k=1}^{d^2} P_k \rho^{R_1Q_1} P_k \left| \sum_{k=1}^{d^2} P_k \rho^{R_2Q_2} P_k \right) - \text{Tr}(\rho^{R_1Q_1} \ln(\rho^{R_2Q_2})) \right)
= -D(p||q) - \text{Tr}(\rho^{R_1Q_1} \ln(\rho^{R_2Q_2})),
\]

where

\[
S(\rho||\sigma) = \text{Tr}(\rho \ln(\rho)) - \text{Tr}(\rho \ln(\sigma))
\]

is the quantum relative entropy, in Eq. (14) we have used the fact that a trace-preserving completely positive transformation reduces the quantum relative entropy (see Refs. [6, 7], p. 47 in Ref. [8]),

\[
p = [p_1 \cdots p_{d^2}],
q = [q_1 \cdots q_{d^2}],
p_k = \langle k^{RQ}|\rho^{R_1Q_1}|k^{RQ} \rangle,
q_k = \langle k^{RQ}|\rho^{R_2Q_2}|k^{RQ} \rangle,
\]

and \( D(\cdots||\cdots) \) is the classical relative entropy given by

\[
D(p||q) = \sum_{k=1}^{d^2} p_k \ln \left( \frac{p_k}{q_k} \right).
\]

Let

\[
g(p, q) = D \{ [p, (1-p)] || [q, (1-q)] \}.
\]

Then

\[
D(p||q) - g(p_1, q_1) = \sum_{k=2}^{d^2} p_k \ln \left( \frac{p_k}{q_k} \right) - (1-p_1) \ln \left( \frac{1-p_1}{1-q_1} \right)
= \sum_{k=2}^{d^2} p_k \ln \left( \frac{p_k(1-q_1)}{q_k(1-p_1)} \right)
\geq \sum_{k=2}^{d^2} p_k \left( 1 - \frac{q_k(1-p_1)}{p_k(1-q_1)} \right)
= 0,
\]

where in Eq. (25), we have used the fact that for \( x > 0 \), \( \ln(x) \geq 1 - 1/x \), with equality if and only if \( x = 1 \). Hence, the equality condition for Eq. (26) is

\[
\frac{q_k}{p_k} = \frac{1-q_1}{1-p_1}, \quad k = 2, \cdots, d.
\]
More general lower bounds to the classical relative entropy are given by Blahut in Ref. [9]. Substituting Eq. (26) into Eq. (15), we get

\[
S(\rho, \mathcal{E}) \leq -g \left[ F(\rho, \mathcal{E}), q_1 \right] - \text{Tr} \left[ \rho^{R_1Q_1} \ln(\rho^{R_2Q_2}) \right],
\]

(28)

where we have used the fact that \( p_1 = F(\rho, \mathcal{E}) \). There are different choices of the \( \rho^{R_2Q_2} \) possible to give different upper bounds on \( S(\rho, \mathcal{E}) \). We consider a few such choices below.

### 3 Special Cases

Let

\[
\rho^{R_2Q_2} = \sum_{k=1}^d \gamma_k |k^R\rangle \langle k^R| \otimes \rho^{Q_2},
\]

(29)

where \( \gamma = [\gamma_1 \cdots \gamma_d] \) is a probability vector, and we have not yet specified the state \( \rho^{Q_2} \). This choice yields

\[
q_1 = \sum_{i,j,k=1}^d \sqrt{\lambda_i \lambda_j} \gamma_k \langle i^Q | \langle i^Q \rangle (|k^R \rangle \langle k^R| \otimes \rho^{Q_2} ) |j^R\rangle |j^Q \rangle
\]

\[
= \sum_{i,j,k=1}^d \sqrt{\lambda_i \lambda_j} \gamma_k \delta_{i,k} \delta_{j,k} \langle i^Q | \rho^{Q_2} | j^Q \rangle
\]

\[
= \sum_{k=1}^d \gamma_k \lambda_k \langle k^Q \rho^{Q_2} | k^Q \rangle,
\]

(30)

(31)

(32)

where \( \delta_{i,k} = 1 \) if \( i = k \) and is zero otherwise. Using Eq. (28), we get

\[
S(\rho, \mathcal{E}) \leq -g(F(\rho, \mathcal{E}), q_1) - \sum_{k=1}^d \lambda_k \ln(\gamma_k) - \text{Tr} \left( \mathcal{E}(\rho) \ln(\rho^{Q_2}) \right),
\]

(33)

where we have used \( \rho^{Q_1} = \mathcal{E}(\rho) \). Again, different choices of \( \rho^{Q_2} \) are possible. Let us consider

\[
\rho^{Q_2} = \sum_{k=1}^d \xi_k |k^Q\rangle \langle k^Q|,
\]

(34)

where \( \xi = [\xi_1 \cdots \xi_d] \) is a probability vector. With this choice and noting that

\[
- \text{Tr} \left[ \mathcal{E}(\rho) \ln(\rho^{Q_2}) \right] = - \sum_k \ln(\xi_k) \langle k^Q \mathcal{E}(\rho) |k^Q \rangle
\]

\[
\leq - \ln(\min_i \{\xi_i\}).
\]

(35)

(36)
Eq. (33) reduces to
\[
S(\rho, \mathcal{E}) \leq -g \left( F(\rho, \mathcal{E}), \sum_{k=1}^{d} \lambda_k \gamma_k \xi_k \right) - \sum_{k=1}^{d} \lambda_k \ln(\gamma_k) - \ln(\min_i \{\xi_i\}) \tag{37}
\]
\[
= H(F(\rho, \mathcal{E})) + \ln \left( \frac{\sum_{i=1}^{d} \lambda_i \gamma_i \xi_i}{\min_i \{\xi_i\}} \right) + (1 - F(\rho, \mathcal{E})) \ln \left( \frac{1}{\sum_{i=1}^{d} \lambda_i \gamma_i \xi_i} - 1 \right) - \sum_{k=1}^{d} \lambda_k \ln(\gamma_k), \tag{38}
\]
where \(H(\cdots)\) is given by Eq. (3).

The QFI follows as a special case by substituting \(\gamma_k = \xi_k = 1/d, k = 1, \ldots, d\). Note that the above inequality holds for any probability vectors \(\gamma\) and \(\xi\). We get the following simpler bound than Eq. (38) by choosing \(\xi_k = 1/d, k = 1, \ldots, d\),
\[
S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + \ln \left( \sum_{i=1}^{d} \lambda_i \gamma_i \right) + (1 - F(\rho, \mathcal{E})) \ln \left( \frac{d}{\sum_{i=1}^{d} \lambda_i \gamma_i} - 1 \right) - \sum_{k=1}^{d} \lambda_k \ln(\gamma_k). \tag{39}
\]
Eqs. (28), (33), (38), and (39) are various Fano-like bounds that can be made tighter by appropriately choosing \(\rho^{R_2Q_2}, \{\gamma, \rho^{Q_2}\}, \{\gamma, \xi\}, \) and \(\gamma\) respectively.

It might seem that one could get away from the dependence of the bounds on \(\lambda\) by making the following choice of \(\rho^{R_2Q_2}\), which is different from Eq. (29). Let \(\beta_k, k = 1, \ldots, d^2\), be the eigenvalues of \(\rho^{R_2Q_2}\) and \(|\psi^{RQ}\rangle\) be one of the eigenvectors of \(\rho^{R_2Q_2}\). Let \(\beta_{\max} = \max_k \beta_k, \beta_{\min} = \min_k \beta_k\). Since the maximum of \(g(F, x), x \in [\beta_{\min}, \beta_{\max}]\) occurs at the end-points, hence to make the bound tighter, one could choose the eigenvalue corresponding to the eigenvector \(|\psi^{RQ}\rangle\) as either \(\beta_{\min}\) or \(\beta_{\max}\). The bound in Eq. (28) can be simplified to
\[
S(\rho, \mathcal{E}) \leq -g(F(\rho, \mathcal{E}), q_1) - \ln(\beta_{\min}), \tag{40}
\]
where \(q_1 = \beta_{\max}\) or \(q_1 = \beta_{\min}\). Suppose \(q_1 = \beta_{\max}\), then to tighten the bound, one could choose \(\beta_{\min}\) as large as possible, or
\[
\beta_{\min} = \frac{1 - \beta_{\max}}{d^2 - 1}. \tag{41}
\]
Substituting in Eq. (40), we get
\[
S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) - F(\rho, \mathcal{E}) \ln \left( \frac{1}{\beta_{\max}} - 1 \right) + \ln(d^2 - 1). \tag{42}
\]
We get the tightest bound by choosing minimum value of \(\beta_{\max}\) given by \(\beta_{\max} = 1/d^2\), which reduces Eq. (42) to the QFI.

If \(q_1 = \beta_{\min}\), then Eq. (40) reduces to
\[
S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + [1 - F(\rho, \mathcal{E})] \ln \left( \frac{1}{\beta_{\min}} - 1 \right). \tag{43}
\]
We get the tightest bound by choosing maximum value of \(\beta_{\min}\) given by \(\beta_{\min} = 1/d^2\), which reduces Eq. (43) to the QFI. Hence, this choice of \(\rho^{R_2Q_2}\) offers no improvement over the QFI.
4  An Example

We compute the QFI and the proposed inequality in Eq. (39) for the depolarizing channel for a single qubit \((d = 2)\) given by

\[
\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z),
\]

where \(X, Y, Z\) are Pauli matrices. Let

\[
\rho = U \begin{pmatrix} \lambda & 0 \\ 0 & 1 - \lambda \end{pmatrix} U^\dagger,
\]

where \(U\) is a randomly chosen \(2 \times 2\) Unitary matrix. It is easy to show that for any choice of \(U\)

\[
F(\rho, \mathcal{E}) = 1 + p\left(\lambda^2 - \lambda - \frac{1}{2}\right),
\]

\[
S(\rho, \mathcal{E}) = H_S(\hat{\lambda}),
\]

where \(H_S(\cdots)\) is the Shannon entropy, \(\hat{\lambda} = [p\lambda/2, (1 - \lambda)p/2, -p/4 + 1/2 + \theta/4, -p/4 + 1/2 - \theta/4]\), and

\[
\theta = \sqrt{p^2 + 12p^2\lambda(1 - \lambda) + 4(1 - p) - 16p\lambda(1 - \lambda)}.
\]

In Fig. 1 we compare \(S(\rho, \mathcal{E})\) with the QFI and the inequality in Eq. (39) numerically optimized over \(\gamma\) to give the tightest bound for \(\lambda = 0.1\). The figure shows that the latter bound is tighter than the QFI. In Fig. 2 we plot the numerically computed value of \(\gamma_1\) that gives the tightest bound in Eq. (39). The QFI corresponds to \(\gamma_1 = 1/d = 0.5\).
References

[1] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, Hoboken, NJ, USA, 2nd edition, 2006.

[2] B. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54:2614–2628, Oct. 1996.

[3] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[4] M. Hayashi. *Quantum Information: An Introduction*. Springer, 2006.

[5] T. S. Han and S. Verdú. Generalizing the Fano inequality. *IEEE Trans. Inf. Theory*, 40:1247–1251, July 1994.

[6] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40:147–151, June 1975.

[7] A. Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Commun. Math. Phys.*, 54:21–32, Feb. 1977.

[8] M. Ohya and D. Petz. *Quantum Entropy and its use*. Springer-Verlag, Berlin, 1st edition, 1993.

[9] R. E. Blahut. Information bounds of the Fano-Kullback type. *IEEE Trans. Inf. Theory*, 22:410–421, July 1976.

Figure 1: Plots of $S(\rho, E)$, the tightest bound from Eq. (39), and the QFI.
Figure 2: $\gamma_1$ that gives the tightest bound in Eq. (39).