

Data Processing Inequalities for the Quantum Guesswork

Ilyass Mejdoub, Julien Béguinot, and Olivier Rioul
LTCL, Télécom Paris, Institut Polytechnique de Paris, France
{firstname.lastname}@telecom-paris.fr

Abstract—Quantum guesswork has emerged as a crucial measure in assessing the distinguishability of nonorthogonal quantum states. In this paper, we review and compare previous definitions of the quantum guesswork, and establish the pre and post data processing inequalities (DPis) that are relevant for the guessing problem. We also derive improved lower and upper bounds on the quantum guesswork in terms of the Shannon entropy and Holevo’s information.

I. INTRODUCTION

The classical guessing game is as follows. Alice has access to the realization $X = x$ of a discrete random variable $X \in \mathcal{X} = \{x_1, \dots, x_n\}$, and Bob asks questions of the form “is $X = x_i$?” to Alice until the answer is “yes”. Both Alice and Bob know the alphabet $\mathcal{X}$ and the probability distribution p_X of X . Bob’s *guessing strategy* specifies the order of the successive guesses he makes until Alice confirms that Bob has found the correct value. A sound strategy never asks twice for the same value of x ; therefore, Bob’s strategy can be seen as a permutation $\sigma \in \mathcal{S}_n$ of the alphabet of cardinality n , where $\sigma(1)$ is the first guess, $\sigma(2)$ is the second, and so on until the secret x is found in at most n trials.

The *guesswork* is the average number of Bob’s guesses under his strategy σ , given by

$$\mathcal{G}_\sigma(X) \triangleq \sum_{i=1}^n i \cdot p_X(\sigma(i)). \quad (1)$$

This quantity is minimized for Bob’s optimal strategy σ^* , such that the probabilities $p_X(\sigma^*(i))$ are in descending order, yielding a so-called *guessing entropy*, introduced by Massey [1]:

$$G(X) = \min_{\sigma \in \mathcal{S}_n} \mathcal{G}_\sigma(X) = \mathcal{G}_{\sigma^*}(X) = \sum_{i=1}^n i \cdot p_X^\downarrow(x_i) \quad (2)$$

where $p_X^\downarrow(x)$ are the probabilities $p_X(x)$ sorted in descending order.

Should Bob gain supplementary side information correlated with X , his resulting guesswork is, on average, lower. In the presence of some side information Y (taking values in an arbitrary alphabet $\mathcal{Y}$), Bob’s strategy depends on his observed value $Y = y$:

$$\sigma : y \in \mathcal{Y} \mapsto \sigma_y \in \mathcal{S}_n. \quad (3)$$

and the corresponding guesswork given observation $Y = y$ is

$$\mathcal{G}_\sigma(X|Y = y) = \sum_{i=1}^n i \cdot p_{X|Y}(\sigma_y(i)|y). \quad (4)$$

Bob’s *conditional guesswork* is the average guesswork over all possible observations:

$$\mathcal{G}_\sigma(X|Y) = \mathbb{E}_Y \sum_{i=1}^n i \cdot p_{X|Y}(\sigma_Y(i)|Y). \quad (5)$$

Now for a given strategy, all observations $y \in \mathcal{Y}$ such that $\sigma_y = \sigma$ yield the same permutation σ , and regrouping terms in the sum gives

$$\begin{aligned} \mathcal{G}_\sigma(X|Y) &= \sum_{y \in \mathcal{Y}} \sum_{i=1}^n i \cdot p_{X,Y}(\sigma_y(i), y) \\ &= \sum_{\sigma \in \mathcal{S}_n} \sum_{i=1}^n i \cdot p_{X,\sigma_Y}(\sigma(i), \sigma) \\ &= \mathcal{G}_\sigma(X|\sigma_Y). \end{aligned} \quad (6)$$

This means that for a fixed strategy $\sigma : y \in \mathcal{Y} \mapsto \sigma_y \in \mathcal{S}_n$, the conditional guesswork depends on the observation Y *only through* σ_Y . As shown by Arikan [2] in 1996, the optimal strategy σ_y^* still consists in guessing in descending order of conditional probabilities $p_{X|Y}(x|y)$, and the *conditional guessing entropy* is the average guesswork for such an optimal strategy σ^* :

$$G(X|Y) = \min_{\sigma} \mathcal{G}_\sigma(X|Y) = \mathcal{G}_{\sigma^*}(X|Y) = \mathbb{E}_Y \sum_{i=1}^n i \cdot p_{X|Y}^\downarrow(x_i|y) \quad (7)$$

where $p_{X|Y}^\downarrow(x|y)$ are the probabilities $p_{X|Y}(x|y)$ sorted in descending order.

If we now substitute the classical random variable Y with quantum side information, we get the notion of *quantum guesswork* introduced by Chen *et al.* [3] as an optimization criterion for discriminating non-orthogonal quantum states. This constitutes an alternative to the conventional error probability criterion [4]–[9]. Furthermore, as mentioned in [10, § IX], quantum guesswork can serve as a security criterion in some quantum information processing tasks such as certifying the safety of an exchanged key in an imperfect implementation of a QKD protocol.

In this quantum guessing game, Alice still has a random variable X whose probability distribution p_X and alphabet $\mathcal{X}$ are known to both parties. Now, when Alice observes the realization $X = x$, she sends Bob a quantum state ρ_x . The quantum ensemble

$$\mathcal{E} \triangleq \{(\rho_x, p_X(x))\}_{x \in \mathcal{X}} \quad (8)$$

is known to both Alice and Bob. The quantum states $\{\rho_x\}_{x \in \mathcal{X}}$ can be either pure or mixed states and belong to the set of density matrices in some finite dimensional Hilbert space $\mathcal{H}$.

Once again, Bob can only ask questions of the form “is $X = x$?”. The only way for Bob to get any helpful information from the received state ρ_x is to eventually measure it. Bob can freely manipulate the state ρ_x , including applying unitary transformations or conducting measurements, to correctly infer the realization x . The most general form of quantum measurement [11], [12] is called POVM (positive operator valued measure) and is mathematically defined as a set $E = \{E_y\}_{y \in \mathcal{Y}}$ of positive semi-definite operators which sum to the identity:

$$E_y \geq 0 \text{ and } \sum_{y \in \mathcal{Y}} E_y = I. \quad (9)$$

The POVM and the quantum ensemble used by Bob define a classical random variable Y_E taking values in $\mathcal{Y}$. By Born’s rule [11], [12]:

$$p_{Y_E|X}(y|x) = \text{Tr}[E_y \rho_x]. \quad (10)$$

so that $p_{Y_E}(y) = \sum_{x \in \mathcal{X}} \text{Tr}[E_y \rho_x] \cdot p_X(x)$. While the channel $X \rightarrow \rho_X$ is quantum, for a fixed POVM E the composition of channels

$$X \rightarrow \boxed{\text{Quantum Channel}} \rightarrow \rho_X \rightarrow \boxed{\text{POVM}} \rightarrow Y_E$$

forms a classical channel. Hence, subject to the POVM E , we can define the quantum conditional guesswork for a given strategy σ as a classical conditional guesswork (6)

$$\mathcal{G}_\sigma(X|Y_E) = \mathcal{G}_\sigma(X|\sigma_{Y_E}) \quad (11)$$

The guesswork depends on ρ_x only through Y_E , and as above, it depends on Y_E only through σ_{Y_E} , according to the following Markov chain

$$X \rightarrow \rho_X \rightarrow \boxed{\text{POVM}} \rightarrow Y_E \rightarrow \sigma_{Y_E}.$$

The quantum guessing entropy is now the minimum average guesswork, achieved for the optimal guess strategy *and* the optimal *measurement* strategy (through the choice of the POVM). Therefore, a natural definition is the following:

Definition 1 (Quantum Guesswork): The *quantum conditional guessing entropy* of X (also named *quantum guesswork*) given a quantum ensemble $\mathcal{E}$ is defined by

$$G(X|\mathcal{E}) = \min_{\sigma, E} \mathcal{G}_\sigma(X|Y_E)$$

The optimization is over the pair (σ, E) ; however, it only depends on σ_{Y_E} so that the procedure can be simplified.

In the present literature on quantum guessing, the quantum guesswork $G(X|\mathcal{E})$ was defined in two ways, either by minimizing a classical guessing entropy over the choice of a POVM E [3], [10], [13], or through its “operational” point of view advocated in [14]–[17]. The equivalence between these two definitions of quantum guesswork is perhaps known in certain circles but, to the best of our knowledge, has not yet been explicitly proved.

The remainder of this paper is organized as follows. In Section II, we restate the two previous definitions of quantum guesswork and formally show that they are equivalent to our Definition 1. In addition, we review and explain anew known results about the measurement attaining the quantum guesswork. The main results of this paper are in Section III. We first establish the unitary invariance property (§ III-A). We then generalize two data processing inequalities to the quantum setting (pre-DPI in § III-C and post-DPI in § III-B). Finally, in § III-D, we propose a general methodology to obtain lower and upper bounds on quantum guesswork in terms of the Shannon entropy and Holevo’s information that improves the bound of Chen *et al.* [3].

II. DEFINITIONS

A. Notations

- $\mathcal{H}$ denotes an arbitrary finite dimensional Hilbert space;
- $\mathcal{L}(\mathcal{H})$ denotes the space of linear operators from $\mathcal{H}$ to $\mathcal{H}$;
- $\mathcal{S}_n$ denotes the set of permutations on $\{1, \dots, n\}$;
- For a permutation $\sigma \in \mathcal{S}_n$, $\bar{\sigma}(i) \triangleq \sigma(n+1-i)$;
- For a normal matrix $A \in \mathcal{L}(\mathcal{H})$ whose spectral decomposition is $A = \sum_{k=1}^d \lambda_k |\psi_k\rangle \langle \psi_k|$, we use the notation $f(A) \triangleq \sum_{k=1}^d f(\lambda_k) |\psi_k\rangle \langle \psi_k|$. In particular,

$$|A| \triangleq \sum_{k=1}^d |\lambda_k| |\psi_k\rangle \langle \psi_k|, \quad (12)$$

$$\mathbb{1}_{A \in S} \triangleq \sum_{k: \lambda_k \in S} |\psi_k\rangle \langle \psi_k|.$$

- *Loewner order:* For Hermitian matrices A, B , we write $A \geq B$ if $A - B$ is positive;
- $\|\cdot\|$ denotes the trace norm $\|A\| \triangleq \text{Tr}(|A|)$;

B. Quantum Guesswork: Chen *et al.*’s Definition $G_1(X|\mathcal{E})$

The first previous definition of the quantum guesswork $G_1(X|\mathcal{E})$ given in [3], [10], [13] is as follows. From the joint distribution $p_X(x)p_{Y_E|X}(y|x)$ of X and Y_E , we compute the (classical) *guessing entropy* $G(X|Y_E)$ from the POVM E and the ensemble $\mathcal{E}$. Bob can now only control the choice of the POVM to minimize his average number of guesses. Thus the quantum guesswork is here defined as

$$G_1(X|\mathcal{E}) \triangleq \inf_E G(X|Y_E). \quad (13)$$

As shown in [10, Theorem 1], the most general quantum measurement strategy Bob can use is either one of the following strategies:

- perform a single measurement using an arbitrary POVM and then apply the classical guessing strategy;
- perform a single measurement using a POVM indexed by permutations $\sigma \in \mathcal{S}_n$ specifying the order of the successive guesses;
- perform successive measurements using POVMs indexed by the remaining possible values using Alice’s feedback to each of Bob’s guesses.

C. Quantum Guesswork: Dall'Arno et al.'s Definition $G_2(X|\mathcal{E})$

The second previous definition of the quantum guesswork $G_2(X|\mathcal{E})$ given in [14]–[17] is as follows. Without loss of generality, we can assume $\mathcal{X} = \{1, \dots, n\}$, and we restrict ourselves to special types of POVMs E indexed by *permutations*:

$$E = \{E_\sigma\}_{\sigma \in \mathcal{S}_n} \quad (14)$$

whose outcome is *operational* in the sense that it gives Bob directly its entire ranking of guesses in the form of a permutation $\sigma \in \mathcal{S}_n$ where $\sigma(i)$ is Bob's i -th guess.

The probability that the outcome of Bob's measurement is σ and that his i -th guess is the correct one (i.e. $\sigma(i) = x$) given that he received the state ρ_x is obtained by Born's rule

$$p(\sigma, i) = \text{Tr}[E_\sigma \cdot \rho_{\sigma(i)}] \cdot p_X(\sigma(i)). \quad (15)$$

If we marginalize over σ we get the probability that the i -th guess is correct given that the received state is ρ_x ,

$$p(i) = \sum_{\sigma \in \mathcal{S}_n} \text{Tr}[E_\sigma \cdot \rho_{\sigma(i)}] \cdot p_X(\sigma(i)). \quad (16)$$

Bob's guesswork for ensemble $\mathcal{E}$ and POVM E is now

$$\mathcal{G}(\mathcal{E}, E) \triangleq \sum_{i=1}^n i \cdot p(i), \quad (17)$$

where the values $p(i)$ are not necessarily in decreasing order, and the quantum guesswork is defined as its minimum over all POVMs $E = \{E_\sigma\}_{\sigma \in \mathcal{S}_n}$:

$$G_2(X|\mathcal{E}) \triangleq \inf_E \mathcal{G}(\mathcal{E}, E). \quad (18)$$

D. Equivalence Between Definitions $G_1(X|\mathcal{E})$ and $G_2(X|\mathcal{E})$

Theorem 1: Definitions of Chen et al. and Dall'Arno et al. are equivalent to our Definition 1:

$$G_1(X|\mathcal{E}) = G_2(X|\mathcal{E}) = G(X|\mathcal{E}). \quad (19)$$

Proof: By definition of conditional guessing entropy,

$$G(X|Y_E) = \min_{\sigma} \mathcal{G}_{\sigma}(X|Y_E) = \mathcal{G}_{\sigma^*}(X|Y_E) \quad (20)$$

where the optimal strategy σ^* is such that for each y , the probabilities $p_{X|Y_E}(\sigma_Y^*(i)|y)$ are sorted in descending order. It follows that

$$G(X|\mathcal{E}) = \min_E \min_{\sigma} \mathcal{G}_{\sigma}(X|Y_E) = \min_E G(X|Y_E) = G_1(X|\mathcal{E}). \quad (21)$$

Now let $\sigma : y \in \mathcal{Y} \mapsto \sigma_y$ be Bob's (not necessarily optimal) strategy and recall the Markov chain

$$\rho_x \rightarrow \boxed{\text{POVM}} \rightarrow Y_E \rightarrow \sigma_{Y_E}$$

and the definition

$$\mathcal{G}_{\sigma}(X|Y_E) = \sum_y \sum_i i \cdot p_{X,Y_E}(\sigma_y(i), y) \quad (22)$$

where by Born's rule,

$$p_{X,Y_E}(x, y) = p_X(x) \cdot \text{Tr}[E_y \rho_x]. \quad (23)$$

Again grouping terms in y corresponding to the same $\sigma_y = \sigma$, we have

$$p_{X,\sigma_{Y_E}}(x, \sigma) = p_X(x) \sum_{y|\sigma_y=\sigma} \text{Tr}[E_y \rho_x] = p_X(x) \text{Tr}[\tilde{E}_{\sigma} \rho_x] \quad (24)$$

where

$$\tilde{E}_{\sigma} = \sum_{y|\sigma_y=\sigma} E_y. \quad (25)$$

is another POVM $\tilde{E}$, indexed by permutations $\sigma \in \mathcal{S}_n$, since $\tilde{E}_{\sigma} \geq 0$ and $\sum_{\sigma} \tilde{E}_{\sigma} = I$. The output of a measurement is now a realization of a random permutation $\Sigma \triangleq Y_{\tilde{E}} \in \mathcal{S}_n$, which directly gives Bob's strategy, where

$$\begin{aligned} \mathcal{G}_{\sigma}(X|Y_E) &= \mathcal{G}_{\text{Id}}(X|\Sigma) \\ &= \sum_{\sigma} \sum_i i \cdot p_{X,\Sigma}(\sigma(i), \sigma) \\ &= \sum_{\sigma} \sum_i i \cdot p(i, \sigma) = \sum_i i \cdot p(i) \end{aligned} \quad (26)$$

where Id is the identity permutation since by construction, $\Sigma = \sigma \iff \sigma_{Y_{\tilde{E}}} = \sigma$. Thus, minimizing over $\tilde{E}$ is the same as minimizing over both E and σ . Therefore,

$$G(X|\mathcal{E}) = \min_E \min_{\sigma} \mathcal{G}_{\sigma}(X|Y_E) = \min_{\tilde{E}} \mathcal{G}_{\text{Id}}(X|\Sigma) = G_2(X|\mathcal{E}) \quad (27)$$

which ends the proof. $\blacksquare$

E. Remarks on Attaining the Minimum

Dall'Arno et al. [14] found a closed form expression $G(X|\mathcal{E})$ under some conditions on the quantum ensemble $\mathcal{E}$, using his definition $G_2(X|\mathcal{E})$ above. For convenience write E instead of $\tilde{E}$, and let

$$\mathcal{G}(\mathcal{E}, E) \triangleq \mathcal{G}_{\text{Id}}(X|\Sigma) \quad (28)$$

to stress the dependence on the quantum ensemble $\mathcal{E}$ and the POVM E . With that definition, the objective function to be minimized over the space of POVMs is

$$\mathcal{G}(\mathcal{E}, E) = \sum_{i=1}^n i \cdot \sum_{\sigma \in \mathcal{S}_n} \text{Tr}[E_{\sigma} \cdot \rho_{\sigma(i)}] \cdot p_X(\sigma(i)) \quad (29)$$

$$= \sum_{\sigma} \text{Tr}[E_{\sigma} \cdot f_{\sigma}] \quad (30)$$

where $f_{\sigma} \triangleq \sum_{i=1}^n i \cdot p_X(\sigma(i)) \rho_{\sigma(i)}$. To simplify this expression consider its evaluation on $\bar{\sigma}$:

$$f_{\bar{\sigma}} = (n+1)\hat{\rho} - f_{\sigma} \quad (31)$$

where $\hat{\rho} \triangleq \sum_{i=1}^n \rho_{\sigma(i)} p_X(\sigma(i))$ does not depend on σ . Therefore, defining

$$\begin{aligned} \mathcal{E}_{\sigma} &\triangleq 2f_{\sigma} - (n+1)\hat{\rho} \\ &= \sum_{i=1}^n (2t - n - 1) p_X(\sigma(i)) \cdot \rho_{\sigma(i)}. \end{aligned} \quad (32)$$

we have

$$\begin{aligned}\mathcal{G}(\mathcal{E}, E) &= \frac{n+1}{2} + \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma} \cdot \mathcal{E}_{\sigma}] \\ &= \frac{n+1}{2} - \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma} \cdot \mathcal{E}_{\bar{\sigma}}]\end{aligned}\quad (33)$$

since $\mathcal{E}_{\bar{\sigma}} = -\mathcal{E}_{\sigma}$.

We need the following lemma.

Lemma 1: Let A be an Hermitian positive matrix. If X and Y are Hermitian matrices such that $X \leq Y$, then $\text{Tr}[AX] \leq \text{Tr}[AY]$.

Proof: Let $Y - X = \sum_{i=1}^d \lambda_i |\varphi_i\rangle \langle \varphi_i|$ be the spectral decomposition of $Y - X \geq 0$. Then

$$\text{Tr}[AY] - \text{Tr}[AX] = \text{Tr}[A(Y - X)] \quad (34)$$

$$= \text{Tr}\left[A \sum_{i=1}^d \lambda_i |\varphi_i\rangle \langle \varphi_i|\right] \quad (35)$$

$$= \sum_{i=1}^d \lambda_i \text{Tr}[\underbrace{|\varphi_i\rangle \langle \varphi_i| A |\varphi_i\rangle}_{\geq 0}] \geq 0 \quad \blacksquare$$

Applying Lemma 1 to $|\mathcal{E}_{\sigma}| \geq \mathcal{E}_{\bar{\sigma}}$ we obtain

$$\mathcal{G}(\mathcal{E}, E) \geq \frac{n+1}{2} - \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma} \cdot |\mathcal{E}_{\bar{\sigma}}|] \quad (36)$$

where we have used Lemma 1. Now, if there exists $\sigma^* \in S_n$ such that $|\mathcal{E}_{\sigma^*}| \geq |\mathcal{E}_{\sigma}|$ for all $\sigma \in S_n$, then

$$\begin{aligned}\mathcal{G}(\mathcal{E}, E) &\geq \frac{n+1}{2} - \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma} \cdot |\mathcal{E}_{\sigma^*}|] \\ &= \frac{n+1}{2} - \frac{1}{2} \text{Tr}[|\mathcal{E}_{\sigma^*}|]\end{aligned}\quad (37)$$

since $\sum_{\sigma} E_{\sigma} = I$. Now

$$-|\mathcal{E}_{\sigma^*}| = \mathbb{1}_{\mathcal{E}_{\sigma^*} < 0} \mathcal{E}_{\sigma^*} - \mathbb{1}_{\mathcal{E}_{\sigma^*} > 0} \mathcal{E}_{\sigma^*} = E_{\sigma^*}^{\sigma^*} \mathcal{E}_{\sigma^*} + E_{\sigma^*}^{\sigma^*} \mathcal{E}_{\sigma^*}^{\sigma^*} \quad (38)$$

where E^{σ^*} is the POVM defined by

$$E_{\sigma}^{\sigma^*} = \begin{cases} \mathbb{1}_{\mathcal{E}_{\sigma} < 0} + \frac{1}{2} \mathbb{1}_{\mathcal{E}_{\sigma} = 0} & \text{if } \sigma \in \{\sigma^*, \bar{\sigma}^*\}, \\ 0 & \text{otherwise.} \end{cases} \quad (39)$$

Indeed, one easily checks that $E_{\sigma}^{\sigma^*} \geq 0$, $\sum_{\sigma} E_{\sigma}^{\sigma^*} = E_{\sigma^*}^{\sigma^*} + E_{\sigma^*}^{\sigma^*} = \mathbb{1}_{\mathcal{E}_{\sigma^*} < 0} + \frac{1}{2} \mathbb{1}_{\mathcal{E}_{\sigma^*} = 0} + \mathbb{1}_{\mathcal{E}_{\sigma^*} < 0} + \frac{1}{2} \mathbb{1}_{\mathcal{E}_{\sigma^*} = 0} = \mathbb{1}_{\mathcal{E}_{\sigma^*} > 0} + \mathbb{1}_{\mathcal{E}_{\sigma^*} < 0} + \mathbb{1}_{\mathcal{E}_{\sigma^*} = 0} = I$. It follows that

$$\mathcal{G}(\mathcal{E}, E) \geq \frac{n+1}{2} + \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma}^{\sigma^*} \cdot \mathcal{E}_{\sigma}] \quad (40)$$

Hence $\mathcal{G}(X|\Sigma)$ is minimized for $E = E^{\sigma^*}$. This explains why this particular POVM achieves the minimum guessing work Dall'Arno et al.'s result:

Theorem 2 ([16, Theorem 1]): if $\exists \sigma^* \in S_n$ s.t. $\forall \sigma \in S_n$ $|\mathcal{E}_{\sigma^*}| \geq |\mathcal{E}_{\sigma}|$ then

$$G(X|\mathcal{E}) = \frac{n+1}{2} + \frac{1}{2} \sum_{\sigma} \text{Tr}[E_{\sigma}^{\sigma^*} \cdot \mathcal{E}_{\sigma}] \quad (41)$$

This closed form formula is only valid under the condition $|\mathcal{E}_{\sigma^*}| \geq |\mathcal{E}_{\sigma}|$. In particular, every ensemble made of uniformly

distributed qubits satisfies this hypothesis [16]. However since the Loewner order $A \geq B$ is not total, the permutation σ^* in Theorem 2 does not always exist, and the problem of efficient computation of the quantum guesswork is still open for many classes of ensembles.

III. DATA PROCESSING INEQUALITIES

A. Unitary Invariance

In the framework of the guessing game, if a unitary transformation is applied to the quantum ensemble, we expect the value of quantum guesswork to remain the same:

Theorem 3: Let U be a unitary matrix and define

$$U\mathcal{E}U^{\dagger} = \{U\rho_x U^{\dagger}, p_X(x)\}_{x \in X}. \quad (42)$$

Then

$$G(X|\mathcal{E}) = G(X|U\mathcal{E}U^{\dagger}). \quad (43)$$

Proof: First observe that $\tilde{E}_y \triangleq U^{\dagger} E_y U$ forms a POVM since $\sum_y \tilde{E}_y = U^{\dagger} \sum_y E_y U = U^{\dagger} U = I$. From the identity

$$\text{Tr}[E_y \cdot U\rho_i U^{\dagger}] = \text{Tr}[U^{\dagger} E_y U \cdot \rho_i], \quad (44)$$

it is easily seen that

$$\mathcal{G}(U\mathcal{E}U^{\dagger}, E) = \mathcal{G}(\mathcal{E}, U^{\dagger} E U). \quad (45)$$

Therefore, since the map $E \mapsto \tilde{E} = U^{\dagger} E U$ is one-to-one,

$$G(X|U\mathcal{E}U^{\dagger}) = \inf_E \mathcal{G}(U\mathcal{E}U^{\dagger}, E) \quad (46)$$

$$= \inf_E \mathcal{G}(\mathcal{E}, U^{\dagger} E U) \quad (47)$$

$$= \inf_{\tilde{E}} \mathcal{G}(\mathcal{E}, \tilde{E}) \quad (48)$$

$$= G(X|\mathcal{E}) \quad \blacksquare$$

B. Post Data Processing Inequality

More generally, assume that a quantum channel is applied to the quantum ensemble. We expect that guessing the label of the output of the quantum channel is more difficult than directly guessing the initial state. This is a generalization of the *data processing inequality* for guesswork $G(X|Y)$ to the quantum case:

Theorem 4: Let $\mathcal{N}$ be a quantum channel (a completely positive trace-preserving map) and define

$$\mathcal{N}(\mathcal{E}) = \{\mathcal{N}(\rho_x), p_X(x)\}_{x \in X}. \quad (49)$$

Then

$$G(X|\mathcal{E}) \leq G(X|\mathcal{N}(\mathcal{E})) \quad (50)$$

Proof: Let

$$\mathcal{N}(\rho_x) = \sum_{l=1}^d V_l \rho_x V_l^{\dagger} \quad (51)$$

be the operator-sum representation [11, Theorem 4.4.1] of $\mathcal{N}$, where $\sum_{l=1}^d V_l^{\dagger} V_l = I$. Since

$$\text{Tr}[E_y \cdot \mathcal{N}(\rho_{x_i})] = \text{Tr}[E_y \cdot \sum_{l=1}^d V_l \rho_{x_i} V_l^{\dagger}] = \text{Tr}[\sum_{l=1}^d V_l^{\dagger} E_y V_l \cdot \rho_{x_i}], \quad (52)$$

one has

$$\mathcal{G}(\mathcal{N}(\mathcal{E}), E) = \mathcal{G}(\mathcal{E}, \tilde{\mathcal{N}}(E)) \quad (53)$$

where $\tilde{\mathcal{N}}(E_y) = \sum_{l=1}^d V_l^\dagger E_y V_l \geq 0$ is a POVM since

$$\sum_y \tilde{\mathcal{N}}(E_y) = \sum_{l=1}^d V_l^\dagger \sum_y E_y V_l = \sum_{l=1}^d V_l^\dagger V_l = I. \quad (54)$$

Therefore,

$$G(X|\mathcal{N}(\mathcal{E})) = \inf_E \mathcal{G}(\mathcal{N}(\mathcal{E}), E) = \inf_E \mathcal{G}(\mathcal{E}, \tilde{\mathcal{N}}(E)) \quad (55)$$

$$\geq \inf_E \mathcal{G}(\mathcal{E}, E) \quad (56)$$

$$= G(X|\mathcal{E}) \quad \blacksquare$$

Remark 1: Note that equality does not hold in general since $E \mapsto \tilde{\mathcal{N}}(E)$ is not always one-to-one. However, one recovers Theorem 3 by applying Theorem 4 twice, once for the channel $\rho \mapsto U\rho U^\dagger$ and once for the inverse channel $\rho \mapsto U^\dagger \rho U$.

C. Pre Data Processing Inequality

Here we use the concept of *majorization* [18]. We say that a random variable Z majorizes X if its distribution p_Z majorizes p_X and we write $X \preceq Z$.

Theorem 5: $G(X|\mathcal{E})$ is Schur-concave, i.e.,

$$X \preceq Z \implies G(X|\mathcal{E}) \geq G(Z|\mathcal{E}). \quad (57)$$

Proof: By Schur-concavity of guessing entropy and conditional guessing entropy [19, Theorem 5], [20], we get

$$X \preceq Z \implies G(Z|Y_E) \leq G(X|Y_E) \quad (58)$$

$$\implies \inf_E G(Z|Y_E) \leq \inf_E G(X|Y_E) \quad (59)$$

$$\implies G(Z|\mathcal{E}) \leq G(X|\mathcal{E}). \quad \blacksquare$$

Since X majorizes $f(X)$ [20], we have the following

Corollary 1: For a deterministic function f , we have

$$G(f(X)|\mathcal{E}) \leq G(X|\mathcal{E}) \quad (60)$$

Guessing a function of X (e.g., its least or most significant bit) is obviously easier than guessing X directly.

D. From Classical to Quantum Guessing vs. Entropy

Closed-form solutions to the quantum guesswork problem are only known for some specific ensembles under certain conditions (geometrically uniform states [3, Section 5], qubits under a uniform distribution [14, Corollary 1] [16, Section B]). When closed-form solutions are not available, it may be desirable to obtain tight upper and lower bounds in terms of the Shannon entropy of X and quantities such as Holevo's information, which can be computed from the quantum ensemble $\mathcal{E}$. In the following, we generalize the approach of [3] to obtain lower and upper bounds from any type of classical inequalities between $H(X|Y)$ and $G(X|Y)$.

Let X and Y_E be two random variables defined as in § I. *Accessible information*, denoted $I_{acc}(\mathcal{E})$, is the maximum amount of information that Bob can extract from his received state ρ_x about X , defined as

$$I_{acc}(\mathcal{E}) \triangleq \sup_E I(X : Y_E). \quad (61)$$

There is no known formula to analytically solve the optimization problem in the definition of accessible information, but we have the following tight upper [21] and lower [22] bounds:

$$\Lambda(\mathcal{E}) \leq I_{acc}(\mathcal{E}) \leq \chi(\mathcal{E}). \quad (62)$$

Here $\chi(\mathcal{E})$ (Holevo's information) and $\Lambda(\mathcal{E})$ are defined by

$$\chi(\mathcal{E}) = S\left(\sum_x p_X(x)\rho_x\right) - \sum_x p_X(x)S(\rho_x) \quad (63)$$

$$\Lambda(\mathcal{E}) = Q\left(\sum_x p_X(x)\rho_x\right) - \sum_x p_X(x)Q(\rho_x) \quad (64)$$

where S denotes the Von Neumann entropy and Q denotes the subentropy, a quantity introduced in [22]:

$$S(\rho) = -\sum_k \lambda_k \log(\lambda_k) \quad (65)$$

$$Q(\rho) = -\sum_k \prod_{l \neq k} \frac{\lambda_k}{\lambda_k - \lambda_l} \lambda_k \log(\lambda_k) \quad (66)$$

where the λ_k 's are the eigenvalues of ρ .

Theorem 6: Let φ and ψ be two non-decreasing functions such that for Shannon's entropy and the classical guessing entropy,

$$\psi(H(X|Y)) \geq G(X|Y) \geq \varphi(H(X|Y)). \quad (67)$$

Then for the quantum guesswork, we have

$$\psi(H(X) - \Lambda(\mathcal{E})) \geq G(X|\mathcal{E}) \geq \varphi(H(X) - \chi(\mathcal{E})). \quad (68)$$

Proof: For any POVM E , we have

$$\psi(H(X|Y_E)) \geq G(X|Y_E) \geq \varphi(H(X|Y_E)). \quad (69)$$

Now, using the bounds in (62),

$$H(X) - \Lambda(\mathcal{E}) \geq \inf_E H(X|Y_E) \geq H(X) - \chi(\mathcal{E}). \quad (70)$$

Taking the infimum over E in (69) we obtain

$$\psi(H(X) - \Lambda(\mathcal{E})) \geq G(X|\mathcal{E}) \geq \varphi(H(X) - \chi(\mathcal{E})). \quad (71)$$

since φ and ψ are non-decreasing. $\blacksquare$

Using the classical McEliece-Yu inequality [23] we recover the upper bound on the quantum guesswork obtained in [3, Thm 3]. In this case McEliece-Yu inequality cannot be improved since it is achieved everywhere when the channel $X \rightarrow Y$ is the n -ary erasure channel.

Using the classical Massey inequality [1] we recover [3, Thm 2]. With Rioul's inequality [24, Eq. 13], we obtain the improved inequality

$$G(X|\mathcal{E}) \geq \frac{2^{H(X) - \chi(\mathcal{E})}}{e} + \frac{1}{2}. \quad (72)$$

Since the above Theorem is generic it can also be used with other improved bounds, e.g., those obtained in [25].

ACKNOWLEDGMENT

The authors are thankful to Michele Dall'Arno for the numerous exchanged emails and his help in understanding the basic theory of quantum guesswork.

REFERENCES

- [1] J. L. Massey, "Guessing and entropy," in *Proceedings of 1994 IEEE International Symposium on Information Theory*. IEEE, 1994, p. 204.
- [2] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 99–105, 1996.
- [3] W. Chen, Y. Cao, H. Wang, and Y. Feng, "Minimum guesswork discrimination between quantum states," *Quantum Information and Computation*, Vol.15, 2015.
- [4] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, pp. 231–252, 1969.
- [5] A. Chefles, "Quantum state discrimination," *Contemporary Physics*, vol. 41, no. 6, pp. 401–424, 2000.
- [6] S. M. Barnett and S. Croke, "Quantum state discrimination," *Advances in Optics and Photonics*, vol. 1, no. 2, pp. 238–278, 2009.
- [7] E. Davies, "Information and quantum measurement," *IEEE Transactions on Information Theory*, vol. 24, no. 5, pp. 596–599, 1978.
- [8] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 858–872, 2001.
- [9] S. M. Barnett, "Minimum-error discrimination between multiply symmetric states," *Physical Review A*, vol. 64, no. 3, p. 030303, 2001.
- [10] E. P. Hanson, V. Katariya, N. Datta, and M. M. Wilde, "Guesswork with quantum side information," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 322–338, 2021.
- [11] M. M. Wilde, *Quantum information theory*. Cambridge university press, 2013.
- [12] J. Watrous, *The theory of quantum information*. Cambridge university press, 2018.
- [13] V. Katariya, N. Bhusal, and C. You, "Experimental Guesswork with Quantum Side Information Using Twisted Light," *Sensors*, vol. 23, no. 14, p. 6570, 2023.
- [14] M. Dall'Arno, F. Buscemi, and T. Koshiha, "Guesswork of a quantum ensemble," *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 3139–3143, 2022.
- [15] B. Avirmed, K. Niinomi, and M. Dall'Arno, "Adversarial guesswork with quantum side information," *Quantum Information and Computation* 23, 1105, 2023.
- [16] M. Dall'Arno, "On the Measurement attaining the Quantum Guesswork," *IEEE Transactions on Information Theory*, 2023.
- [17] M. Dall'Arno, F. Buscemi, and T. Koshiha, "Computing the quantum guesswork: a quadratic assignment problem," *Quantum Information and Computation*, vol. 23, no. 9&10, pp. 0721–0732, 2023.
- [18] A. W. Marshall, I. Olkin, and B. Arnold, *Inequalities: Theory of Majorization and Its Applications*, 2nd ed., ser. Springer Series in Statistics. Springer, 2011.
- [19] J. Béguinot, W. Cheng, S. Guillely, and O. Rioul, "Be my guess: Guessing entropy vs. success rate for evaluating side-channel attacks of secure chips," in *2022 25th Euromicro Conference on Digital System Design (DSD)*. IEEE, 2022, pp. 496–503.
- [20] O. Rioul, "The interplay between error, total variation, alpha-entropy and guessing: Fano and Pinsker direct and reverse inequalities," *Entropy*, vol. 25, no. 7, p. 978, 2023.
- [21] A. S. Holevo, "Statistical problems in quantum physics," in *2nd Japan-USSR Symposium on Probability Theory*, ser. Lecture Notes in Mathematics, G. Maruyama and Y. Prokhorov, Eds., vol. 330. Springer, 1973, pp. 104–119. [Online]. Available: <https://api.semanticscholar.org/CorpusID:124959629>
- [22] R. Jozsa, D. Robb, and W. K. Wootters, "Lower bound for accessible information in quantum mechanics," *Physical Review A*, vol. 49, no. 2, p. 668, 1994.
- [23] R. J. McEliece and Z. Yu, "An inequality on entropy," in *Proc. IEEE International Symposium on Information Theory*, 1995, p. 329.
- [24] O. Rioul, "Variations on a Theme by Massey," *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 2813–2828, 2022.
- [25] J. Béguinot and O. Rioul, "What can information guess? Guessing advantage vs. Rényi entropy for small leakages," in *IEEE International Symposium on Information Theory, ISIT 2024, Athens, Greece, July 7-12, 2024*. IEEE, 2024, pp. 2963–2968. [Online]. Available: <https://doi.org/10.1109/ISIT57864.2024.10619150>