Quantum Information and Computation, Vol. 23, No. 13&14 (2023) 1105–1118

ADVERSARIAL GUESSWORK WITH QUANTUM SIDE INFORMATION

BAASANCHIMED AVIRMED
Department of Computer Science and Engineering, Toyohashi University of Technology
1-1 Hibarigaoka, Tempaku-cho, Toyohashi, Aichi, 441-8580, Japan

KAITO NIINOMI
Department of Computer Science and Engineering, Toyohashi University of Technology
1-1 Hibarigaoka, Tempaku-cho, Toyohashi, Aichi, 441-8580, Japan

MICHELE DALL'ARNO
Department of Computer Science and Engineering, Toyohashi University of Technology
1-1 Hibarigaoka, Tempaku-cho, Toyohashi, Aichi, 441-8580, Japan
michele.dallarno.mv@tut.jp

Received August 25, 2023
Revised October 14, 2023

The guesswork of a classical-quantum channel quantifies the cost incurred in guessing the state transmitted by the channel when only one state can be queried at a time, maximized over any classical pre-processing and minimized over any quantum post-processing. For arbitrary-dimensional covariant classical-quantum channels, we prove the invariance of the optimal pre-processing and the covariance of the optimal post-processing. In the qubit case, we compute the optimal guesswork for the class of so-called highly symmetric informationally complete classical-quantum channels.

Keywords: Quantum guesswork, quantum ensemble, quantum measurement, quantum hypothesis testing, quantum state discrimination, quadratic assignment problem

1 Introduction

Let us first introduce an adversarial extension of the usual guesswork problem in the absence of side information [1–10]. One party, say Alice, is free to choose a probability distribution p for a random variable M over alphabet $\mathcal{M}$, and to communicate her choice to the other party, say Bob (in the previously considered, non-adversarial scenario, p is fixed by the rules of the game). At each round of the game, Alice picks a value m for variable M at random according to distribution p, and Bob queries Alice for the values of random variable M, one at a time, until his guess is correct. For instance, let us consider the case $\mathcal{M} = \{a, b, c\}$. In this case, Bob's first query could be, say, b. If Alice answers on the negative, then his next query could be a. Assuming this time Alice answers on the affirmative, the round is over.

Bob chooses the order of his queries in order to minimize the cost incurred, the cost function being known to both parties in advance and only depending on the average number of queries; Alice chooses the prior probability distribution p to maximize such a cost. The optimal strategies for both Alice and Bob are obvious: for Alice it consists of choosing p as the uniform distribution over $\mathcal{M}$, while for Bob it consists of querying the values of M in non-increasing order of their prior probability.

Let us now introduce the adversarial extension of the guesswork problem in the presence of side information [11–15], that, most generally, is quantum (again, the quantum cases so far considered were not adversarial, that is, the prior p was assumed fixed by the rules). That is, let us now say that there is a communication channel $\boldsymbol{\sigma}$ with random variable M as input and quantum states as output (a classical-quantum, or c-q, channel for short), known to both parties. Suppose also that, at each round of the game, Bob is given a state $\boldsymbol{\sigma}(m)$.

How would the optimal strategies for both parties look like in this case? Bob is free to perform the most general quantum measurement on his state in order to get a posterior probability distribution on M, and queries Alice based on such a posterior (it was shown in Ref. [15] that more general strategies that make use of Alice's feedback after each query do not help); Alice chooses the prior in order to antagonize such an optimal strategy. In this case, therefore, the optimal strategies on both sides are not obvious at all and depend on the c-q channel $\boldsymbol{\sigma}$.

In this work, after formalizing the problem of the adversarial guesswork with quantum side information in Section 2, we address the arbitrary dimensional case (Section 3.1). We prove that the order in which Alice and Bob choose their strategies in irrelevant (Lemma 1); that each choice of strategy amounts to a convex problem (Lemma 2); that any symmetry of $\boldsymbol{\sigma}$, if any, implies an analog symmetry of Alice's and Bob's optimal strategies (Lemma 3); and that Bob's optimal strategy amounts to querying the values of M in decreasing order of their posterior probability distribution (Lemma 4).

Then, we specify to the qubit case (Section 3.2). Using the fact, shown in Ref. [15], that the optimization of Bob's strategy can be reframed as a combinatorial problem known as quadratic assignment [16–21], we derive a branch and bound [22–24] (BB) algorithm for the closed-form computation of the guesswork (Theorem 1). We apply such an algorithm to compute the closed-form expression of the guesswork of the highly-symmetric, informationally-complete (HSIC) c-q channels introduced in Ref. [25] (Corollary 1), and we provide an implementation with the IBM quantum computer of the optimal guesswork protocol for the icosidodecahedral HSIC channel. We summarize our results and discuss some open problems in Section 4.

2 Formalization

We use standard definitions and results in quantum information theory [26].

For any finite-dimensional Hilbert space $\mathcal{H}$ we denote with $\mathcal{L}_+(\mathcal{H})$ the cone of positive semidefinite operators on $\mathcal{H}$.

For any finite set $\mathcal{M}$ we define the set $\mathcal{D}_\mathcal{M}$ of probability distributions over $\mathcal{M}$ given by

$$\mathcal{D}_\mathcal{M} := \left\{ p : \mathcal{M} \to [0,1] \,\middle|\, \sum_{m \in \mathcal{M}} p\left(m\right) = 1 \right\},$$

the set $\mathcal{C}(\mathcal{M}, \mathcal{H})$ of c-q channels given by

$$\mathcal{C}\left(\mathcal{M}, \mathcal{H}\right) := \left\{ \boldsymbol{\sigma} : \mathcal{M} \to \mathcal{L}_+\left(\mathcal{H}\right) \,\middle|\, \mathrm{Tr}\left[\boldsymbol{\sigma}\left(\cdot\right)\right] = 1 \right\},$$

the set $\mathcal{N}_\mathcal{M}$ of numberings of $\mathcal{M}$ given by

$$\mathcal{N}_\mathcal{M} := \left\{ \mathbf{n} : \{1, \ldots, |\mathcal{M}|\} \to \mathcal{M} \,\middle|\, \mathbf{n} \text{ bijective} \right\},$$

and the set $\mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ of numbering-valued measurements given by

$$\mathcal{P}\left(\mathcal{N}_{\mathcal{M}}, \mathcal{H}\right) := \left\{ \boldsymbol{\pi} : \mathcal{N}_{\mathcal{M}} \to \mathcal{L}_{+}\left(\mathcal{H}\right) \middle| \sum_{\mathbf{n} \in \mathcal{N}_{\mathcal{M}}} \boldsymbol{\pi}\left(\mathbf{n}\right) = \mathbb{1} \right\}.$$

For any finite set $\mathcal{M}$, any finite dimensional Hilbert space $\mathcal{H}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$, we denote with $p_{\boldsymbol{\sigma},\boldsymbol{\pi}}$ the probability distribution that the outcome of $\boldsymbol{\pi}$ is $\mathbf{n}$ and the t-th query is correct, that is

$$\begin{aligned} p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}} &: \mathcal{N}_{\mathcal{M}} \times \{1, \dots, |\mathcal{M}|\} \to [0,1] \\ (\mathbf{n}, t) &\mapsto p\left(\mathbf{n}\left(t\right)\right) \operatorname{Tr}\left[\boldsymbol{\pi}\left(\mathbf{n}\right) \boldsymbol{\sigma}\left(\mathbf{n}\left(t\right)\right)\right], \end{aligned}$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ and any $t \in \{1, \dots, |\mathcal{M}|\}$. We denote with $q_{\boldsymbol{\sigma},\boldsymbol{\pi}}$ the probability distribution that the t-th guess is correct, obtained marginalizing $p_{\boldsymbol{\sigma},\boldsymbol{\pi}}$, that is

$$\begin{aligned} q_{p,\boldsymbol{\sigma},\boldsymbol{\pi}} &: \{1, \dots, |\mathcal{M}|\} \to [0,1] \\ t &\mapsto \sum_{\mathbf{n} \in \mathcal{N}_{\mathcal{M}}} p_{\boldsymbol{\sigma},\boldsymbol{\pi}}\left(\mathbf{n}, t\right), \end{aligned}$$

For any cost function $\gamma : \{1, \dots, |\mathcal{M}|\}$, the guesswork $G^{\gamma} : \mathcal{D}_{\mathcal{M}} \times \mathcal{C}(\mathcal{M}, \mathcal{H}) \times \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H}) \to \mathbb{R}$ is given by

$$\begin{aligned} &G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\pi}\right) \\ :=& \sum_{\substack{t \in \{1, \dots, |\mathcal{M}|\} \\ \mathbf{n} \in \mathcal{N}_{\mathcal{M}}}} p\left(\mathbf{n}\left(t\right)\right) \operatorname{Tr}\left[\boldsymbol{\sigma}\left(\mathbf{n}\left(t\right)\right) \boldsymbol{\pi}\left(\mathbf{n}\right)\right] \gamma\left(t\right), \end{aligned}$$

for any probability distribution $p \in \mathcal{D}_{\mathcal{M}}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$.

The minimum guesswork $G^{\gamma}_{\min} : \mathcal{D}_{\mathcal{M}} \times \mathcal{C}(\mathcal{M}, \mathcal{H}) \to \mathbb{R}$ is given by

$$G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma}\right) := \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\pi}\right),$$

for any probability distribution $p \in \mathcal{D}_{\mathcal{M}}$ and any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and the maximin guesswork $G^{\gamma}_{\max\min} : \mathcal{C}(\mathcal{M}, \mathcal{H}) \to \mathbb{R}$ is given by

$$G^{\gamma}_{\max\min}\left(\boldsymbol{\sigma}\right) := \max_{p \in \mathcal{D}_{\mathcal{M}}} G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma}\right), \tag{1}$$

for any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$.

The maximum guesswork $G^{\gamma}_{\max} : \mathcal{C}(\mathcal{M}, \mathcal{H}) \times \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H}) \to \mathbb{R}$ is given by

$$G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\pi}\right) := \max_{p \in \mathcal{D}_{\mathcal{M}}} G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\pi}\right),$$

for any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$ and any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$, and the minimax guesswork $G^{\gamma}_{\min\max} : \mathcal{C}(\mathcal{M}, \mathcal{H}) \to \mathbb{R}$ given by

$$G^{\gamma}_{\min\max}\left(\boldsymbol{\sigma}\right) := \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\pi}\right), \tag{2}$$

for any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$.

3 Main results

3.1 Arbitrary dimensional case

The following lemma shows that, without loss of generality, we can focus on the maximin guesswork $G^{\gamma}_{\max\min}$ only.

Lemma 1 (Maximin)**.** *For any finite set $\mathcal{M}$, any finite-dimensional Hilbert space $\mathcal{H}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any function $\gamma : \{1, \ldots, |\mathcal{M}|\}$, the maximin guesswork $G^{\gamma}_{\max\min}(\boldsymbol{\sigma})$ and the minimax guesswork $G^{\gamma}_{\min\max}(\boldsymbol{\sigma})$ are equivalent, that is*

$$G^{\gamma}_{\max\min}(\boldsymbol{\sigma}) = G^{\gamma}_{\min\max}(\boldsymbol{\sigma})$$

Proof. The statement immediately follows from von Neumann's minimax theorem by observing that the set $\mathcal{D}_{\mathcal{M}}$ of probability distributions and the set $\mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ of numbering-valued measurements are compact and that the guesswork $G^{\gamma}(\cdot, \boldsymbol{\rho}, \cdot)$ is bilinear over such sets. □

Next, we prove the convexity and the covariance of the maximization problem over probability distributions in the right hand side of Eq. (1) and of the minimization problem over numbering-valued measurements in the right hand side of Eq. (2). Despite sharing these properties, we will show that the former problem is "easy" while the latter problem is "hard", in terms of finding a closed-form solution as well as in terms of complexity class.

The following lemma shows that the maximization problem in the right hand side of Eq. (1) and the minimization problem in the right hand side of Eq. (2) are convex programming problems.

Lemma 2 (Convexity)**.** *For any finite set $\mathcal{M}$, any finite-dimensional Hilbert space $\mathcal{H}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any function $\gamma : \{1, \ldots, |\mathcal{M}|\}$, the minimum guesswork $G^{\gamma}_{\min}(\cdot, \boldsymbol{\sigma})$ is a concave function over the set $\mathcal{D}_{\mathcal{M}}$ of probability distributions and the maximum guesswork $G^{\gamma}_{\max}(\boldsymbol{\sigma}, \cdot)$ is a convex function over the set $\mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ of numbering-valued measurements.*

Proof. The first part of the statement immediately follows by the linearity of G^{γ} over the set $\mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ of numbering-valued measurements. Indeed, for any two probability distributions $p, q \in \mathcal{D}_{\mathcal{M}}$ and any probabilities $\lambda \in [0, 1]$ and $\mu := 1 - \lambda$ one has

$$\begin{aligned}
& G^{\gamma}_{\min}(\lambda p + \mu q, \boldsymbol{\sigma}) \\
= & \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} G^{\gamma}(\lambda p + \mu q, \boldsymbol{\sigma}, \boldsymbol{\pi}) \\
= & \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} \left[\lambda G^{\gamma}(p, \boldsymbol{\sigma}, \boldsymbol{\pi}) + \mu G^{\gamma}(q, \boldsymbol{\sigma}, \boldsymbol{\pi})\right] \\
\geq & \lambda \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} G^{\gamma}(p, \boldsymbol{\sigma}, \boldsymbol{\pi}) + \mu \min_{\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})} G^{\gamma}(q, \boldsymbol{\sigma}, \boldsymbol{\pi}) \\
= & \lambda G^{\gamma}_{\min}(p, \boldsymbol{\sigma}) + \mu G^{\gamma}_{\min}(q, \boldsymbol{\sigma}).
\end{aligned}$$

The second part of the statement immediately follows by the linearity of G^{γ} over the set $\mathcal{D}_{\mathcal{M}}$ of probability distributions. Indeed, for any two numbering-valued measurements

$\boldsymbol{\pi}, \boldsymbol{\tau} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ and any probabilities $\lambda \in [0,1]$ and $\mu := 1 - \lambda$ one has

$$\begin{aligned}
& G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \lambda\boldsymbol{\pi} + \mu\boldsymbol{\tau}\right) \\
= & \max_{p \in \mathcal{D}_{\mathcal{M}}} G^{\gamma}\left(p, \boldsymbol{\sigma}, \lambda\boldsymbol{\pi} + \mu\boldsymbol{\tau}\right) \\
= & \max_{p \in \mathcal{D}_{\mathcal{M}}} \left[\lambda G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\pi}\right) + \mu G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\tau}\right)\right] \\
\leq & \lambda \max_{p \in \mathcal{D}_{\mathcal{M}}} G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\pi}\right) + \mu \max_{p \in \mathcal{D}_{\mathcal{M}}} G^{\gamma}\left(p, \boldsymbol{\sigma}, \boldsymbol{\tau}\right) \\
= & \lambda G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\pi}\right) + \mu G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\tau}\right).
\end{aligned}$$

□

It is relevant to compare the computational complexities of the two problems in the right hand side of Eq. (1) and (2). On the one hand, the size of the problem in the right hand side of Eq. (1) grows linearly with $|\mathcal{M}|$; hence, its computational complexity class is P. On the other hand, the size of the problem in the right hand side of Eq. (2) grows factorially with $|\mathcal{M}|$ (since $|\mathcal{N}_{\mathcal{M}}| = |\mathcal{M}|!$); even in the qubit case, such a problem has been proven [15] to be a particular instance of the quadratic assignment problem [19] (QAP), a well-know NP-hard combinatorial problem.

Let us turn now to the symmetric case. For any finite set $\mathcal{M}$, the symmetric group $\mathcal{S}_{\mathcal{M}}$ is given by

$$\mathcal{S}_{\mathcal{M}} := \left\{ g : \mathcal{M} \to \mathcal{M} \middle| g \text{ bijective} \right\}.$$

For any finite-dimensional Hilbert space $\mathcal{H}$ and any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, we say that a map $R : \mathcal{L}_+(\mathcal{H}) \to \mathcal{L}_+(\mathcal{H})$ is a statistical morphism [27] of $\boldsymbol{\sigma}$ if and only if for any discrete set $\mathcal{N}$ and any measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}, \mathcal{H})$, there exists measurement $\boldsymbol{\tau} \in \mathcal{P}(\mathcal{N}, \mathcal{H})$ such that

$$\mathrm{Tr}\left[\boldsymbol{\pi}\left(n\right) R \circ \boldsymbol{\sigma}\left(m\right)\right] = \mathrm{Tr}\left[\boldsymbol{\tau}\left(n\right) \boldsymbol{\sigma}\left(m\right)\right], \tag{3}$$

for any $m \in \mathcal{M}$ and any $n \in \mathcal{N}$.

For any group $\mathcal{G} \subseteq \mathcal{S}_{\mathcal{M}}$, we say that a c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$ is $\mathcal{G}$-covariant if and only if there exists a representation $\mathcal{R} := \{R_g : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})\}$ of $\mathcal{G}$, where R_g is a statistical morphism of $\boldsymbol{\sigma}$ for any $g \in \mathcal{G}$, such that

$$R_g \circ \boldsymbol{\sigma} = \boldsymbol{\sigma} \circ g. \tag{4}$$

For any group $\mathcal{G} \subseteq \mathcal{S}_{\mathcal{M}}$ and any $\mathcal{G}$-covariant c-q channel $\boldsymbol{\sigma}$, we say that $\mathcal{G}$ is transitive iff there exists one such representation such that its action on $\boldsymbol{\sigma}$ is transitive, and we say that $\boldsymbol{\sigma}$ is centrally symmetric (CS for short) iff there exists one such representation and a $g \in \mathcal{G}$ such that $R_g(\cdot) = 2\mathbb{1}/d - (\cdot)$, where d denotes the Hilbert space dimension, in which case we introduce the short-hand notation $\overline{(\cdot)} := g(\cdot)$.

The following lemma shows that the probability distribution attaining the maximum in the right hand side of Eq. (1) and the numbering-valued measurement attaining the minimum in the right hand side of Eq. (2) share the same symmetries as the c-q channel.

Lemma 3 (Covariant case)**.** *For any finite set $\mathcal{M}$, any finite-dimensional Hilbert space $\mathcal{H}$, any group $\mathcal{G} \subseteq \mathcal{S}_{\mathcal{M}}$, any $\mathcal{G}$-covariant c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any function $\gamma : \{1, \ldots, |\mathcal{M}|\} \to \mathbb{R}$, there exist $\mathcal{G}$-invariant probability distribution $p \in \mathcal{D}_{\mathcal{M}}$ and $\mathcal{G}$-covariant measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ that attain $G^{\gamma}_{\max\min}(\boldsymbol{\sigma})$.*

Proof. Let us prove the first part of the statement. For any probability distribution $p \in \mathcal{D}_{\mathcal{M}}$, upon defining the probability distribution $q \in \mathcal{D}_{\mathcal{M}}$ given by $q := |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} p \circ g$, one has $G^{\gamma}_{\min}(p, \boldsymbol{\sigma}) \leq G^{\gamma}_{\min}(q, \boldsymbol{\sigma})$. This can be seen as follows:

$$\begin{aligned} G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma}\right) &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma} \circ g\right) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\min}\left(p \circ g^{-1}, \boldsymbol{\sigma}\right) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\min}\left(p \circ g, \boldsymbol{\sigma}\right) \\ &\leq G^{\gamma}_{\min}\left(\frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} p \circ g, \boldsymbol{\sigma}\right) \\ &= G^{\gamma}_{\min}\left(q, \boldsymbol{\sigma}\right). \end{aligned}$$

where the first equality follows from the fact that, due to Eqs. (3) and (4), $G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma}\right) = G^{\gamma}_{\min}\left(p, \boldsymbol{\sigma} \circ g\right)$ for any $g \in \mathcal{G}$, the second equality follows by direct inspection, the third equality follows from the group structure of $\mathcal{G}$, the inequality follows from the concavity of the guesswork $G^{\gamma}_{\min}$ in p proven in Lemma 2, and the final equality follows by definition of q. By definition of q it immediately follows that q is invariant under the action of $\mathcal{G}$, that is, for any $g \in \mathcal{G}$ one has $q \circ g = q$.

Let us prove the second part of the statement. For any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{M}, \mathcal{H})$, upon defining the numbering-valued measurement $\boldsymbol{\tau} \in \mathcal{P}(\mathcal{M}, \mathcal{H})$ given by $\boldsymbol{\tau}(\cdot) := |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} R_g^{-1} \circ \boldsymbol{\pi}(g \circ \cdot)$, one has $G^{\gamma}_{\max}(\boldsymbol{\sigma}, \boldsymbol{\pi}) \geq G^{\gamma}_{\max}(\boldsymbol{\sigma}, \boldsymbol{\tau})$.

This can be seen as follows:

$$\begin{aligned} G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\pi}\right) &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\max}\left(R_g^{-1} \circ \boldsymbol{\sigma} \circ g, \boldsymbol{\pi}\right) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, R_g \circ \boldsymbol{\pi}\left(g^{-1} \circ \cdot\right)\right) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, R_g^{-1} \circ \boldsymbol{\pi}\left(g \circ \cdot\right)\right) \\ &\geq G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} R_g^{-1} \circ \boldsymbol{\pi}\left(g \circ \cdot\right)\right) \\ &= G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\tau}\right). \end{aligned}$$

where the first equality follows from the fact that, due to Eqs. (3) and (4), $G^{\gamma}_{\max}\left(\boldsymbol{\sigma}, \boldsymbol{\pi}\right) = G^{\gamma}_{\max}\left(R_g^{-1} \boldsymbol{\sigma} \circ g, \boldsymbol{\pi}\right)$ for any $g \in \mathcal{G}$, the second equality follows by direct inspection, the third equality follows from the group structure of $\mathcal{G}$, the inequality follows from the convexity of the guesswork $G_{\max}$ in $\boldsymbol{\pi}$ proven in Lemma 2, and the final equality follows by definition of $\boldsymbol{\tau}$. By definition of $\boldsymbol{\tau}$ it immediately follows that $\boldsymbol{\tau}$ is covariant under the action of $\mathcal{G}$, that is, for any $g \in \mathcal{G}$ one has $R_g \circ \boldsymbol{\tau} = \boldsymbol{\tau} \circ g$. □

Let us consider the case of a transitive symmetry. In this case, it is possible to provide the closed-form solution to the maximization problem in the right hand side of Eq. (1) by noticing that the only fully invariant probability distribution is the uniform probability distribution; it is not possible however in general to solve in closed-form the minimization problem in the right hand side of Eq. (2) owing to the operatorial structure of measurements.

Having shown that, of the two optimization problems we are considering (maximization over probability distributions and minimization over numbering-valued measurements), the former is "easy" and the latter is "hard" (in the precise meanings discussed above), we focus in the following on the latter.

It will be convenient to restrict to non–increasing cost functions, formalizing the expectation that the cost increases with the number of queries needed to correctly guess. That this restriction comes with no loss of generality can be shown as follows. For any finite set $\mathcal{M}$ and any function $\gamma : \{1, \dots |\mathcal{M}|\} \to \mathbb{R}$, let us define $\overleftarrow{\gamma} := \gamma \circ \sigma$, where $\sigma : \{1, \dots |\mathcal{M}|\} \to \{1, \dots |\mathcal{M}|\}$ is any permutation such that $\overleftarrow{\gamma}$ is non increasing. It immediately follows (see Lemma 2 of Ref. [15]) that, for any finite-dimensional Hilbert space $\mathcal{H}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, and any function $\gamma : \{1, \dots, |\mathcal{M}|\}$, one has

$$G^{\gamma}_{\min}(p, \boldsymbol{\sigma}) = G^{\overleftarrow{\gamma}}_{\min}(p, \boldsymbol{\sigma}).$$

Moreover, if numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{M}, \mathcal{H})$ attains the minimum guesswork $G^{\gamma}_{\min}(p, \boldsymbol{\sigma})$, then numbering-valued measurement $\boldsymbol{\pi}'(\cdot) := \boldsymbol{\pi}(\cdot \circ \sigma^{-1})$ attains the minimum guesswork $G^{\overleftarrow{\gamma}}_{\min}(p, \boldsymbol{\sigma})$. Hence, in the following without loss of generality we may assume whenever needed that the cost function γ is non decreasing.

The following lemma (which generalizes Lemma 4 of Ref. [13] to the case of arbitrary cost function γ) formalizes through Bayes theorem the intuition that, for non decreasing cost function γ, the optimal strategy for Bob implies querying the values of M in the order of their non increasing posterior probability.

Lemma 4 (Bayes)**.** *For any discrete set $\mathcal{M}$, any non decreasing cost function $\gamma : \{1, \dots |\mathcal{M}|\} \to \mathbb{R}$, any probability distribution $p \in \mathcal{D}_{\mathcal{M}}$, any finite dimensional Hilbert space $\mathcal{H}$, and any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, a measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ minimizes the guesswork, that is $G^{\gamma}_{min}(p, \boldsymbol{\sigma}) = G^{\gamma}(p, \boldsymbol{\sigma}, \boldsymbol{\pi})$, only if $p_{\boldsymbol{\rho}, \boldsymbol{\pi}}(\mathbf{n}, \cdot)$ is not increasing for any $\mathbf{n} \in \mathcal{N}(\mathcal{M})$.*

Proof. We show that, for any numbering valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$, there exists a numbering valued measurement $\boldsymbol{\pi}' \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ such that the probability distribution $p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}'}(\mathbf{n}, \cdot)$ is not increasing for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ and $G^{\gamma}(p, \boldsymbol{\sigma}, \boldsymbol{\pi}') \le G^{\gamma}(p, \boldsymbol{\sigma}, \boldsymbol{\pi})$, with equality if and only if $p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}}(\mathbf{n}, \cdot) = p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}'}(\mathbf{n}, \cdot)$ for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Let $\{g_{\mathbf{n}} : \{1, \dots, |\mathcal{M}|\} \to \{1, \dots, |\mathcal{M}|\} \mid g_{\mathbf{n}} \text{ bijective}\}_{\mathbf{n} \in \mathcal{N}_{\mathcal{M}}}$ be a numbering indexed family of permutations such that the probability distribution $p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}}(\mathbf{n}, g_{\mathbf{n}}(\cdot))$ is not increasing for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Let function $f : \mathcal{N}_{\mathcal{M}} \to \mathcal{N}_{\mathcal{M}}$ be given by the composition

$$f(\mathbf{n}) := \mathbf{n} \circ g_{\mathbf{n}},$$

for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Let the numbering valued measurement $\boldsymbol{\pi}' \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})$ be the coarse graining of numbering valued measurement $\boldsymbol{\pi}$ given by

$$\boldsymbol{\pi}'(\mathbf{n}') := \sum_{\mathbf{n} \in f^{-1}[\mathbf{n}']} \boldsymbol{\pi}(\mathbf{n}),$$

for any numbering $\mathbf{n}' \in \mathcal{N}_{\mathcal{M}}$, where $f^{-1}[\mathbf{n}']$ denotes the counter-image of $\mathbf{n}'$ with respect to f. By direct computation, one has that

$$\begin{aligned} q_{\boldsymbol{\sigma},\boldsymbol{\pi}'}(t) &= \sum_{\mathbf{n}' \in \mathcal{N}_{\mathcal{M}}} \sum_{\mathbf{n} \in f^{-1}[\mathbf{n}']} p(\mathbf{n}'(t)) \operatorname{Tr}[\boldsymbol{\sigma}(\mathbf{n}'(t)) \boldsymbol{\pi}(\mathbf{n})] \\ &= \sum_{\mathbf{n} \in \mathcal{N}_{\mathcal{M}}} p(f(\mathbf{n})(t)) \operatorname{Tr}[\boldsymbol{\sigma}(f(\mathbf{n})(t)) \boldsymbol{\pi}(\mathbf{n})] \\ &= \sum_{\mathbf{n} \in \mathcal{N}_{\mathcal{M}}} p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}}(\mathbf{n}, g_{\mathbf{n}}(t)), \end{aligned}$$

for any $t \in \{1, \ldots, |\mathcal{M}|\}$. Therefore, by construction one has that the probability distribution $q_{\boldsymbol{\rho},\boldsymbol{\pi}}$ is majorized by the probability distribution $q_{\boldsymbol{\rho},\boldsymbol{\pi}'}$, that is

$$\sum_{t \in \{1,\ldots,T\}} q_{\boldsymbol{\rho},\boldsymbol{\pi}}(t) \leq \sum_{t \in \{1,\ldots,T\}} q_{\boldsymbol{\rho},\boldsymbol{\pi}'}(t).$$

for any $T \in \{1, \ldots, |\mathcal{M}|\}$, with equality if and only if $p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}}(\mathbf{n}, \cdot) = p_{p,\boldsymbol{\sigma},\boldsymbol{\pi}'}(\mathbf{n}, \cdot)$ for any numbering $\mathbf{n} \in \mathcal{N}(\mathcal{M})$. Therefore, the statement follows. $\square$

3.2 The qubit case

Finally, in this section we show that the maximization over numbering–valued measurements can be solved in closed-form for any given qubit c-q channel, if the probability distribution is uniform and the cost function is balanced. For any finite set $\mathcal{M}$, any non increasing cost function $\gamma : \{1, \ldots |\mathcal{M}|\} \to \mathbb{R}$ is balanced if and only if $\gamma(t) + \gamma(|\mathcal{M}| + 1 - t) = 2\overline{\gamma}$ for any $t \in \{1, \ldots |\mathcal{M}\}$.

Among balanced cost functions, it will be convenient to restrict to those whose average is null. That this restriction comes without loss of generality immediately follows from the fact that

$$G_{\min}^{\gamma}\left(|\mathcal{M}|^{-1}, \sigma\right) = \overline{\gamma} - G_{\min}^{\gamma_0}\left(|\mathcal{M}|^{-1}, \sigma\right),$$

where $\gamma_0 := \gamma - \overline{\gamma}$ has null average.

Before proceeding, we need to define a family of operators that will allow us to reframe the optimization over numbering-valued measurements as a quantum hypothesis testing problem. For any finite set $\mathcal{M}$, any non decreasing balanced cost function $\gamma : \{1, \ldots |\mathcal{M}|\} \to \mathbb{R}$ with null average, any finite-dimensional Hilbert space $\mathcal{H}$, any c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, let $E_{\boldsymbol{\sigma}}^{\gamma}$ be the function given given by

$$E_{\boldsymbol{\sigma}}^{\gamma}(\mathbf{n}) := \frac{2}{|\mathcal{M}|} \sum_{t=1}^{|\mathcal{M}|} \gamma(t) \boldsymbol{\sigma}(\mathbf{n}(t)),$$

for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$.

We are now in a position to introduce a branch and bound [22–24] (BB) algorithm for the closed-form computation of the guesswork of qubit ensembles. A branch and bound algorithm maximizes an objective function over a feasible set by recursively splitting the feasible set into subsets, then minimizing the objective function on such subsets; the splitting is called branching. For each such subset, the algorithm computes a bound on the maximum it is trying to find, and uses such bounds to "prune" the search space, eliminating the subsets that cannot contain an optimal solution.

For any $\mathcal{N} \subseteq \mathcal{N}_{\mathcal{M}}$, let us define

$$t^*_{\mathcal{N}} := \underset{\substack{t \in \mathbb{N} \\ \mathbf{n}(t) = \mathbf{n}'(t),\ \forall \mathbf{n}, \mathbf{n}' \in \mathcal{N}}}{\arg\max} \quad t + 1,$$

and

$$\mathcal{M}^*_{\mathcal{N}} := \mathcal{M} \setminus \begin{cases} \bigcup_{\mathbf{n} \in \mathcal{N}} \left\{ \mathbf{n}\left(t\right), \mathbf{n}\left(|\mathcal{M}| - t\right) \right\}_{t=1}^{t^*_{\mathcal{N}}} & \text{if } \boldsymbol{\sigma} \text{ CS}, \\ \bigcup_{\mathbf{n} \in \mathcal{N}} \left\{ \mathbf{n}\left(t\right) \right\}_{t=1}^{t^*_{\mathcal{N}}} & \text{otherwise}. \end{cases}$$

Definition 1 (BB algorithm)**.** *For any finite set $\mathcal{M}$, any balanced non increasing cost function $\gamma : \{1, \dots \mathcal{M}\} \to \mathbb{R}$ with null average, any two-dimensional Hilbert space $\mathcal{H}$, any group $\mathcal{G} \subseteq \mathcal{S}_{\mathcal{M}}$, and any $\mathcal{G}$-covariant c-q channel $\boldsymbol{\sigma}(\mathcal{M}, \mathcal{H})$, let us define the BB algorithm given by the objective function $\| E^{\gamma}_{\boldsymbol{\sigma}}\left(\cdot\right) \|$, the feasible set $\texttt{branch}^j(\mathcal{N}^{(0)}_{\mathcal{M}})(m)$ for arbitrary $m \in \mathcal{M}$, where $j = 1$ if $\mathcal{G}$ is transitive and $j = 0$ otherwise and*

$$\mathcal{N}^{(0)}_{\mathcal{M}} := \begin{cases} \left\{ \mathbf{n} \in \mathcal{N}_{\mathcal{M}} \middle| \sigma\left(\mathbf{n}\left(\cdot\right)\right) + \sigma\left(\overline{\mathbf{n}}\left(\cdot\right)\right) = \mathbb{1} \right\}, & \text{if } \boldsymbol{\sigma} \text{ is CS}, \\ \mathcal{N}_{\mathcal{M}} & \text{otherwise}, \end{cases}$$

the branching rule

$$\texttt{branch}(\mathcal{N}) := \left\{ \mathcal{N}_m \subseteq \mathcal{N} \middle| \mathbf{n} \in \mathcal{N}_m \Leftrightarrow \mathbf{n}\left(t^*_{\mathcal{N}}\right) = m \right\}_{m \in \mathcal{M}^*_{\mathcal{N}}},$$

and the bounding rule

$$\texttt{bound}(\mathcal{N}) := (k+1) \left(\left\| \sum_{t=1}^{t^*_{\mathcal{N}} - 1} \gamma\left(t\right) \boldsymbol{\sigma}\left(\mathbf{n}\left(t\right)\right) \right\| + \sum_{t = t^*_{\mathcal{N}}}^{\frac{|\mathcal{M}|}{2k}} \gamma\left(t\right) \right), \tag{5}$$

for arbitrary $\mathbf{n} \in \mathcal{N}$, where $k = 1$ if $\boldsymbol{\sigma}$ is CS and $k = 0$ otherwise.

Theorem 1. *For any finite set $\mathcal{M}$, any balanced non increasing cost function $\gamma : \{1, \dots \mathcal{M}\} \to \mathbb{R}$, any two-dimensional Hilbert space $\mathcal{H}$, any group $\mathcal{G} \subseteq \mathcal{S}_{\mathcal{M}}$, and any $\mathcal{G}$-covariant c-q channel $\boldsymbol{\sigma}(\mathcal{M}, \mathcal{H})$, the BB algorithm in Definition 1 computes the closed-form expression of the guesswork $G^{\gamma}_{\min}(|\mathcal{M}|^{-1}, \boldsymbol{\sigma})$ on C computing units in finite time $T_C(\boldsymbol{\sigma})$ given by*

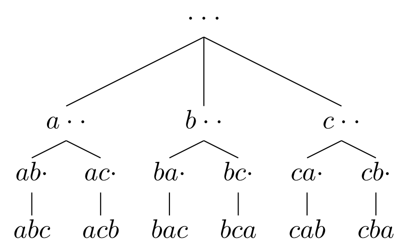
$$T_C\left(\boldsymbol{\sigma}\right) \le \frac{1}{C} \begin{cases} (|\mathcal{M}| - 1)! & \text{if } \mathcal{G} \text{ is transitive}, \\ |\mathcal{M}|!! & \text{if } \mathcal{G} \text{ is CS}, \\ (|\mathcal{M}| - 2)!! & \text{if } \mathcal{G} \text{ is transitive and CS}, \\ |\mathcal{M}|! & \text{otherwise}, \end{cases}$$

where $(\cdot)!!$ denotes the doubly factorial function.

Proof. Due to Theorem 1 and Corollary 1 of Ref. [15] one has

$$G_{\min}^{\gamma}\left(|\mathcal{M}|^{-1},\boldsymbol{\sigma}\right)=-\frac{1}{2}\max_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}}\left\|E_{p,\boldsymbol{\sigma}}^{\gamma}\left(\mathbf{n}^{*}\right)\right\|.$$

As observed in Ref. [15], this represents an instance of the quadratic assignment problem [19] (QAP) that can be solved by a BB algorithm. Permutations can be generated as the leaves of a tree, as shown by the following tree diagram for the case $\mathcal{M}=\{a,b,c\}$.

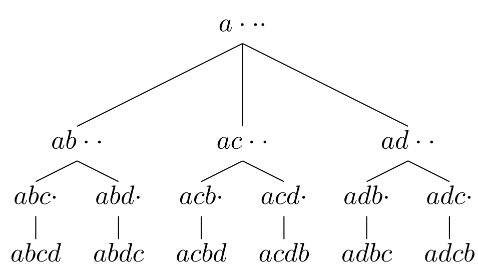


Hence the complexity for the general case is $|\mathcal{M}|!$.

However, in the presence of symmetries this can be improved upon by observing that the operators $E_{p,\boldsymbol{\sigma}}^{\gamma}$'s inherit the covariance of the c-q channel $\boldsymbol{\sigma}$ under the action of the statistical-morphism representation of transitive group $\mathcal{G}$, that is

$$R_g\circ E_{p,\boldsymbol{\sigma}}^{\gamma}=E_{p,\boldsymbol{\sigma}}^{\gamma}\left(g\circ\cdot\right).$$

Hence, if $\mathcal{G}$ is transitive, for any $m\in\mathcal{M}$, there exists an optimal numbering $\mathbf{n}^{*}$ such that $\mathbf{n}^{*}(1)=m^{*}$, for any $m^{*}\in\mathcal{M}$. Permutations satisfying this condition can be generated as the leaves of a tree whose root satisfies the condition, as shown by the following tree diagram, this time for the case $\mathcal{M}=\{a,b,c,d\}$ and $m^{*}=a$.



Hence the complexity in this case is $(|\mathcal{M}|-1)!$.

Moreover, if $\mathcal{G}$ is CS, due to Lemma 4 there exists an optimal numbering $\mathbf{n}^{*}$ such that

$$\boldsymbol{\sigma}\left(\mathbf{n}^{*}\left(\cdot\right)\right)+\boldsymbol{\sigma}\left(\mathbf{n}^{*}\circ\sigma_{\gamma}^{-1}\left(\cdot\right)\right)=\mathbb{1}.$$

Once again, permutations satisfying this condition can be generated as the leaves of a tree if the t-th and the $(|\mathcal{M}|+1-t)$-th states are fixed at each branch, as shown by the following tree diagram, this time for the case $\mathcal{M} = \{a, \bar{a}, b, \bar{b}\}$.

$$
\begin{array}{cccccccc}
 & & & \cdot\cdot\cdot\cdot & & & & \\
\multicolumn{2}{c}{a \cdot\cdot \bar{a}} & \multicolumn{2}{c}{\bar{a} \cdot\cdot a} & \multicolumn{2}{c}{b \cdot\cdot \bar{b}} & \multicolumn{2}{c}{\bar{b} \cdot\cdot b} \\
ab\bar{b}b & a\bar{b}b\bar{a} & \bar{a}b\bar{b}a & \bar{a}\bar{b}ba & ba\bar{a}\bar{b} & b\bar{a}a\bar{b} & \bar{b}a\bar{a}b & \bar{b}\bar{a}ab
\end{array}
$$

Hence the complexity in this case is $|\mathcal{M}|!!$.

Moreover, for a transitive and CS $\mathcal{G}$, combining the two results above the complexity becomes $|\mathcal{M} - 2|!!$, attainable by generating the permutations according to the following tree, again for $\mathcal{M} = \{a, \bar{a}, b, \bar{b}\}$.

$$
\begin{array}{cc}
\multicolumn{2}{c}{a \cdot\cdot \bar{a}} \\
ab\bar{b}b & a\bar{b}b\bar{a}
\end{array}
$$

Finally, each of the trees above represents a so-called embarrassingly parallel problem, that is, the computation in each branch is independent of that in other branches, so the computation in different branches can be assigned to different computing unit with speedup given by the number of such units. $\square$

A parallel implementation in the C programming language of the BB algorithm given by Definition 1 is made available under a free software license [28].

We are now in a position to compute the closed-form expression of the guesswork of highly symmetric, informationally complete (HSIC) qubit c-q channels.

For any finite set $\mathcal{M}$ and any two-dimensional Hilbert space $\mathcal{H}$, a c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$ is highly-symmetric, informationally complete (HSIC) [25] if and only if it is injective and its image $\boldsymbol{\sigma}(\mathcal{M})$ corresponds in the Bloch sphere to a convex regular polyhedron (tetrahedron, octahedron, cube, icosahedron, or dodecahedron), the cuboctahedron, or the icosidodecahedron.

Corollary 1 (Guesswork of HSIC qubit c-q channels)**.** *For any finite set $\mathcal{M}$, any two-dimensional Hilbert space $\mathcal{H}$, and any HSIC c-q channel $\boldsymbol{\sigma} \in \mathcal{C}(\mathcal{M}, \mathcal{H})$, the guesswork $G_{\max\min}(\boldsymbol{\rho})$ for identity cost function $\gamma(\cdot) = \cdot$ is given by*

$$
G_{\max\min}(\boldsymbol{\sigma}) = \begin{cases}
\frac{5}{2} - \frac{\sqrt{15}}{6} \sim 1.9 & |\mathcal{M}| = 4, \\
\frac{7}{2} - \frac{\sqrt{35}}{6} \sim 2.5 & |\mathcal{M}| = 6, \\
\frac{9}{2} - \frac{\sqrt{7}}{2} \sim 3.2 & |\mathcal{M}| = 8, \\
\frac{13}{2} - \frac{\sqrt{110\left(65+29\sqrt{5}\right)}}{60} \sim 4.5 & |\mathcal{M}| = 12, \\
\frac{21}{2} - \frac{\sqrt{6\left(3321+1483\sqrt{5}\right)}}{60} \sim 7.2 & |\mathcal{M}| = 20.
\end{cases}
$$

if $\boldsymbol{\sigma}(\mathcal{M})$ is a regular convex polyhedron,

$$
G_{\max\min}(\boldsymbol{\sigma}) = \frac{13}{2} - \frac{\sqrt{570}}{6} \sim 4.5,
$$

if $\boldsymbol{\sigma}(\mathcal{M})$ is a cuboctahedron, and

$$G_{\max\min}(\boldsymbol{\sigma}) = \frac{31}{2} - \frac{\sqrt{117490 + 52534\sqrt{5}}}{30\sqrt{6 + 2\sqrt{5}}} \sim 10.5,$$

if $\boldsymbol{\sigma}(\mathcal{M})$ is an icosidodecahedron.

Proof. Due to Lemma 3 and the transitivity of $\mathcal{G}$, the probability distribution p attaining the maximin guesswork $G_{\max\min}(\boldsymbol{\sigma})$ is uniform, that is, $p(m) = |\mathcal{M}|^{-1}$ for any $m \in \mathcal{M}$. The guesswork of regular convex polyhedra was derived in Ref. [13]. The guesswork of the cuboctahedron was derived in Ref. [14]. However, the techniques derived therein do not suffice for the computation of the guesswork of the remaining HSIC qubit c-q channel, that is, the icosidodecahedral c-q channel (for which $|\mathcal{M}| = 30$), since the practical application of such techniques is limited to $|\mathcal{M}| \sim 24$. We obtained such a result by applying the BB algorithm in Definition 1, whose computational complexity in this case is $T_C(\boldsymbol{\sigma}) \leq 28!!/C \sim 10^{15}/C$. We initialized the feasible solution using a greedy algorithm (whose complexity is quadratic), whose output turned out to be already within 1% from the optimal solution. For $C = 16$, the computation took around one day. □

Finally, we implemented the minimum guesswork setup for the icosidodecahedral c-q channel and run it on an IBM quantum computer. We generated one circuit for each of the 30 states of the ensemble, and ran 4000 shots for each of the 30 circuits using the `ibmq_quito` backend. The resulting minimum guesswork is $G_{\max\min}(\boldsymbol{\rho}) \sim 10.4$, which is within 1% from the ideal minimum guesswork $G_{\max\min}(\boldsymbol{\rho}) \sim 10.5$ reported in Corollary 1.

4 Conclusion and outlooks

In this work we addressed the problem of the adversarial guesswork in the presence of quantum side information. For the arbitrary-dimensional case, we proved that i) the order in which the strategies of the two parties are optimized is irrelevant, ii) that each optimization corresponds to a convex problem, and that iii) that covariances of the problem, if any, are recast as covariances in the optimal strategies. We conclusively settled the qubit case by deriving a BB algorithm for the computation of the closed-form expression of the guesswork, and we applied it to compute the guesswork of HSIC c-q channels.

The problem of the guesswork for symmetric c-q channels in arbitrary dimension remains open. The difficulty stems from the fact that, while the operators $E^{\gamma}_{p,\boldsymbol{\sigma}}$'s preserve the symmetries of $\boldsymbol{\sigma}$, a (factorially large) number of inequivalent seeds is needed to generate all the $E^{\gamma}_{p,\boldsymbol{\sigma}}$'s from a representation of $\mathcal{G}$, and thus standard techniques for semidefinite programming in the presence of symmetries cannot be applied directly.

All in all, the guesswork represents a relatively new and unexplored operational quantifier of information. As such, it has promising applications in contexts such as information-disturbance relations, where it could potentially be used in place of well-established quantifiers of information such as the mutual information; in majorization theory, where operational concepts such as the testing regions, typically defined in terms of error probability, could be redefined in terms of guesswork; in quantum cryptographic applications, where bounding the guesswork of a communication channel could allow for alternative security proofs; in witnessing the violation of Bell inequalities; finally, the application of the guesswork could be extended from c-q channels to encompass quantum channels and quantum combs.

Acknowledgments

M. D. is grateful to Alessandro Bisio and Francesco Buscemi for insightful discussions. M. D. acknowledges support from the Department of Computer Science and Engineering, Toyohashi University of Technology, from the International Research Unit of Quantum Information, Kyoto University, and from the JSPS KAKENHI grant number JP20K03774.

References

1. J. Massey, *Guessing and entropy*, Proceedings of 1994 IEEE International Symposium on Information Theory, 204 (1994).
2. E. Arikan, *An inequality on guessing and its application to sequential decoding*, IEEE Trans. Inform. Theory **42**, 99 (1996).
3. E. Arikan and N. Merhav, *Guessing subject to distortion*, IEEE Trans. Inform. Theory **44**, 1041 (1998).
4. E. Arikan and N. Merhav, *Joint source-channel coding and guessing with application to sequential decoding*, IEEE Trans. Inform. Theory **44**, 1756 (1998).
5. D. Malone and W. Sullivan, *Guesswork and Entropy*, IEEE Trans. Inform. Theory **50**, 525 (2004).
6. R. Sundaresan, *Guessing Under Source Uncertainty*, IEEE Trans. Inform. Theory **53**, 269 (2007).
7. M. K. Hanawal and R. Sundaresan, *Guessing Revisited: A Large Deviations Approach*, arXiv:1008.1977.
8. M. M. Christiansen and K. R. Duffy, *Guesswork, Large Deviations, and Shannon Entropy*, IEEE Trans. Inform. Theory **59**, 796 (2013).
9. I. Sason and S. Verdú, *Improved Bounds on Lossless Source Coding and Guessing Moments via Rnyi Measures*, arXiv:1801.01265.
10. I. Sason, *Tight Bounds on the Rnyi Entropy via Majorization with Applications to Guessing and Compression*, Entropy **20**, 896 (2018).
11. W. Chen, Y. Cao, H. Wang, Y. Feng, *Minimum guesswork discrimination between quantum states*, Quantum Information & Computation **15**, 0737 (2015).
12. E. P. Hanson, V. Katariya, N. Datta, and M. M. Wilde, *Guesswork with Quantum Side Information*, IEEE Trans. Inform. Theory **68**, 322 (2022).
13. M. Dall'Arno, F. Buscemi, and T. Koshiba, *Guesswork of a quantum ensemble*, IEEE Trans. Inform. Theory **68**, 3193 (2022).
14. M. Dall'Arno, F. Buscemi, and T. Koshiba, *Computing the quantum guesswork: a quadratic assignment problem*, Quantum Information and Computation **23**, 0721 (2023).
15. M. Dall'Arno, *Quantum guesswork*, arXiv:2302.06783.
16. T. C. Koopmans, M. Beckmann, *Assignment problems and the location of economic activities*, Econometrica **25**, 53 (1957).
17. S. Sahni, T. Gonzalez, *P-Complete Approximation Problems*, Journal of the ACM **23**, 555 (1976).
18. G. Laporte and H. Mercure, *Balancing hydraulic turbine runners: A quadratic assignment problem*, European Journal of Operational Research **35**, 378 (1988).
19. E. Dragoti-Çela, *The quadratic assignment problem: Theory and algorithms* (Kluwer Academic Publishers, 1998, Dordrecht, The Netherlands).
20. R. E. Burkard, E. Dragoti-Çela, P. M. Pardalos, and L. S. Pitsoulis, *The Quadratic Assignment Problem*, Handbook of Combinatorial Optimization, Kluwer Academic Publishers, 241 (1998).
21. R. E. Burkard, E. Dragoti-Çela, G. Rote, and G. J. Woeginger, *The quadratic assignment problem with a monotone anti-Monge and a symmetric Toeplitz matrix: Easy and hard cases*, Mathematical Programming **82**, 125 (1998).

22. A. H. Land and A. G. Doig (1960), *An automatic method of solving discrete programming problems*, Econometrica **28**, 497 (1960).
23. J. D. C Little, K. G. Murty, D. W. Sweeney, C. Karel, *An algorithm for the traveling salesman problem*, Operations Research **11**, 972 (1963).
24. J. Clausen, *Branch and Bound Algorithms – Principles and Examples*, Technical report, University of Copenhagen (1999).
25. W. Słomczyński and A. Szymusiak, *Highly symmetric POVMs and their informational power*, Quantum Information Processing **15**, 565 (2016).
26. M. M. Wilde, *Quantum Information Theory*, (Cambridge University Press, 2017).
27. F. Buscemi, *Comparison of quantum statistical models: equivalent conditions for sufficiency*, Commun. Math. Phys. **310**, 625 (2012).
28. B. Avirmed, K. Niinomi, and M. Dall'Arno, *A parallel implementation in the C programming language of a branch and bound algorithm for the computation of the guesswork of any given qubit ensemble*, `https://codeberg.org/mda/gw`.