Guesswork of a Quantum Ensemble

Michele Dall'Arno, Francesco Buscemi, and Takeshi Koshiba, *Member, IEEE*

***Abstract*— The guesswork of a quantum ensemble quantifies the minimum number of guesses needed in average to correctly guess the state of the ensemble, when only one state can be queried at a time. Here, we derive analytical solutions of the guesswork problem subject to a finite set of conditions, including the analytical solution for any qubit ensemble with uniform probability distribution. As explicit examples, we compute the guesswork for any qubit regular polygonal and polyhedral ensemble.**

***Index Terms*— Guesswork, quantum states, quantum measurements, quantum state discrimination.**

I. Introduction

WE CONSIDER a communication scenario involving two parties, Alice and Bob. An ensemble $\boldsymbol{\rho}$ of quantum states with labels in a set $\mathcal{M}$ is given and known to both parties. At each round, Alice picks a label $m \in \mathcal{M}$ with probability $\mathrm{Tr}[\boldsymbol{\rho}(m)]$ and hands state $\mathrm{Tr}[\boldsymbol{\rho}(m)]^{-1}\boldsymbol{\rho}(m)$ over to Bob. Bob aims at correctly guessing label m being allowed to query one element of $\mathcal{M}$ at a time, until his query is correct, at which point the round is over. The cost function incurred by Bob is the average number of guesses, or *guesswork*, until he correctly guesses m. Bob's most general strategy consists of performing a quantum measurement $\boldsymbol{\pi}$ outputing an element $\mathbf{n}$ from the set $\mathcal{N}_{\mathcal{M}}$ of numberings of $\mathcal{M}$ and querying the elements of $\mathcal{M}$ in the order specified by $\mathbf{n}$. Hence, the guesswork is given by the occurence of label m in numbering $\mathbf{n}$, averaged over all numberings. Using the formalism [1] of quantum circuits, the setup is as follows:

$$m \in \mathcal{M} = \boxed{\boldsymbol{\rho}(m)} \overset{\mathcal{H}}{\text{---}} \boxed{\boldsymbol{\pi}(\mathbf{n})} = \mathbf{n} \in \mathcal{N}_{\mathcal{M}}. \quad (1)$$

The guesswork has been extensively studied for classical ensembles [2]–[12], but only very recently tackled for quantum ensembles [13]–[15]. While previous works focused on the derivation of entropic bounds, our aim is instead the derivation of analytical solutions. Our main result, Theorem 1, provides an analytical solution subject to a finite set of conditions. In particular, Corollary 1 provides the analytical solution for any qubit ensemble with uniform probability distribution, thus disproving the conjecture [13] that analytical solutions exist only for binary and symmetric ensembles. As explicit examples, in Corollaries 2 and 3 we explicitly compute the minimum guesswork of any qubit regular polygonal and polyhedral ensebles, respectively. This proves a conjecture [14] on the guesswork of the square qubit ensemble.

II. Formalization

In this section we define the guesswork problem. We use standard results from quantum information theory [1].

First, we introduce the sets of ensembles and numbering-valued measurements that appear in the setup of Eq. (1). For any finite dimensional Hilbert space $\mathcal{H}$, we denote with $\mathcal{L}_+(\mathcal{H})$ the cone of positive semi-definite operators on $\mathcal{H}$. For any finite set $\mathcal{M}$, we denote with $\mathcal{N}_{\mathcal{M}}$ the set of numberings given by

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

We denote with $\mathcal{E}(\mathcal{M}, \mathcal{H})$ the set of ensembles given by

$$\mathcal{E}(\mathcal{M}, \mathcal{H}) := \left\{ \boldsymbol{\rho} : \mathcal{M} \to \mathcal{L}_+(\mathcal{H}) \,\middle|\, \sum_{m \in \mathcal{M}} \mathrm{Tr}[\boldsymbol{\rho}(m)] = 1 \right\}.$$

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

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

Next, we introduce the probability distributions that describe the setup in Eq. (1). For any ensemble $\boldsymbol{\rho}$ and any numbering-valued measurement $\boldsymbol{\pi}$, we denote with $p_{\boldsymbol{\rho},\boldsymbol{\pi}}$ the joint probability distribution that the outcome of $\boldsymbol{\pi}$ is numbering $\mathbf{n}$ and that the t-th guess is correct, that is $\mathbf{n}(t) = m$. In formula:

$$\begin{aligned} p_{\boldsymbol{\rho},\boldsymbol{\pi}} \; &: \mathcal{N}_{\mathcal{M}} \times \{1, \dots, |\mathcal{M}|\} \longrightarrow [0,1] \\ &(\mathbf{n}, t) \longmapsto \mathrm{Tr}\left[\boldsymbol{\rho}(\mathbf{n}(t))\, \boldsymbol{\pi}(\mathbf{n})\right], \end{aligned}$$

Manuscript received December 16, 2020; revised October 15, 2021; accepted January 14, 2022. Date of publication January 26, 2022; date of current version April 21, 2022. The work of Michele Dall'Arno was supported in part by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) under Grant JPMXS0118067285; in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant JP20K03774; and in part by the International Research Unit of Quantum Information, Kyoto University. The work of Francesco Buscemi was supported in part by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) under Grant JPMXS0120319794, in part by MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe" under Grant 21H05183, and in part by JSPS KAKENHI under Grant 19H04066 and Grant 20K03746. The work of Takeshi Koshiba was supported in part by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) under Grant JPMXS0118067285 and Grant JPMXS0120319794; and in part by JSPS KAKENHI under Grant 16H01705, Grant 17H01695, Grant 19K22849, and Grant 21H04879. *(Corresponding author: Michele Dall'Arno.)*

Michele Dall'Arno is with the Yukawa Institute for Theoretical Physics, Kyoto University, Sakyo-ku, Kyoto 606-8502, Japan, and also with the Faculty of Education and Integrated Arts and Sciences, Waseda University, Shinjuku-ku, Tokyo 169-8050, Japan (e-mail: dallarno.michele@yukawa.kyoto-u.ac.jp).

Francesco Buscemi is with the Department of Mathematical Informatics, Graduate School of Informatics, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan (e-mail: buscemi@nagoya-u.jp).

Takeshi Koshiba is with the Faculty of Education and Integrated Arts and Sciences, Waseda University, Shinjuku-ku, Tokyo 169-8050, Japan (e-mail: tkoshiba@waseda.jp).

Communicated by S. Beigi, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2022.3146463

for any $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$ and any $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$. We denote with $q_{\boldsymbol{\rho},\boldsymbol{\pi}}$ the probability distribution that the t-th guess is correct, obtained marginalizing the joint probability distribution $p_{\boldsymbol{\rho},\boldsymbol{\pi}}$. In formula:

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

for any $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$ and any $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$.

Finally, we are in a position to introduce the guesswork. The *guesswork* G is a function mapping any pair $(\boldsymbol{\rho},\boldsymbol{\pi})$ of ensemble and numbering-valued measurement into the expectation value of the number t of guesses, averaged with the probability distribution $q_{\boldsymbol{\rho},\boldsymbol{\pi}}$ of correctness of the t-th guess. In formula:

$$\begin{aligned} G \,:&\mathcal{E}(\mathcal{M},\mathcal{H}) \times \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H}) \longrightarrow [1,\infty) \\ &(\boldsymbol{\rho},\boldsymbol{\pi}) \longmapsto \sum_{t=1}^{|\mathcal{M}|} q_{\boldsymbol{\rho},\boldsymbol{\pi}}\left(t\right) t. \end{aligned}$$

The *minimum guesswork* $G_{\min}$ is a function mapping any ensemble $\boldsymbol{\rho}$ into the minimum over numbering-valued measurements of the guesswork G. In formula:

$$\begin{aligned} G_{\min} \,:&\mathcal{E}(\mathcal{M},\mathcal{H}) \longrightarrow [1,\infty) \\ &\boldsymbol{\rho} \longmapsto \min_{\boldsymbol{\pi}\in\mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})} G\left(\boldsymbol{\rho},\boldsymbol{\pi}\right). \end{aligned}$$

III. Main Results

In this section we derive the analytical solution of the guesswork problem subject to a finite set of conditions, including any qubit ensemble with uniform probability distribution.

In order to state our main result, we need the following definitions. For any finite dimensional Hilbert space $\mathcal{H}$, we denote with $\mathcal{L}(\mathcal{H})$ the space of Hermitian operators on $\mathcal{H}$. For any finite set $\mathcal{M}$ and any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, we denote with $E_{\boldsymbol{\rho}} : \mathcal{N}_{\mathcal{M}} \to \mathcal{L}(\mathcal{H})$ the map given by

$$E_{\boldsymbol{\rho}}\left(\mathbf{n}\right) := \sum_{t=1}^{|\mathcal{M}|} \left(2t - |\mathcal{M}| - 1\right) \boldsymbol{\rho}\left(\mathbf{n}\left(t\right)\right),$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. For any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, we denote with $\overline{\mathbf{n}}$ the reversed numbering. In formula:

$$\overline{\mathbf{n}}\left(t\right) := \mathbf{n}\left(|\mathcal{M}| + 1 - t\right),$$

for any $t \in \{1,\dots,|\mathcal{M}|\}$. We denote with $\Pi_{-}(\cdot)$ and $\Pi_{0}(\cdot)$ the projectors on the negative and null parts of $(\cdot)$, respectively. We denote with $\{\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}})\}_{\mathbf{n}^*\in\mathcal{N}_{\mathcal{M}}}$ the family of numbering-valued measurements given by

$$\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\left(\mathbf{n}\right) := \begin{cases} \left(\Pi_{-} + \frac{1}{2}\Pi_{0}\right)\left(E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\right), & \text{if } \mathbf{n} \in \{\mathbf{n}^*, \overline{\mathbf{n}}^*\}, \\ 0, & \text{otherwise}, \end{cases}$$

for any $\mathbf{n}^*, \mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. It follows from Lemma 1 that the corresponding guesswork is given by

$$G\left(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\right) = \frac{|\mathcal{M}|+1}{2} - \frac{1}{2}\left\|E_{\boldsymbol{\rho}}\left(\mathbf{n}^*\right)\right\|_1, \tag{2}$$

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

Upon denoting with $|\cdot|$ the absolute value of operator $(\cdot)$, the following theorem provides analytical solutions of the minimum guesswork problem subject to a finite set of conditions.

Theorem 1: For any finite set $\mathcal{M}$, any finite dimensional Hilbert space $\mathcal{H}$, and any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, if there exists numbering $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ such that

$$\left|E_{\boldsymbol{\rho}}\left(\mathbf{n}^*\right)\right| \geq E_{\boldsymbol{\rho}}\left(\mathbf{n}\right), \tag{3}$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, then numbering-valued measurement $\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$ minimizes the guesswork, that is

$$G_{\min}\left(\boldsymbol{\rho}\right) = G\left(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\right).$$

We remark that, while the minimum guesswork problem is by definition an optimization over a *continuous* set, the conditions given by Eq. (3) are *finite* in number and hence can be checked by exhaustive search. If they hold, Eq. (2) provides the analytical solution of the minimum guesswork problem.

Proof: Due to Lemma 1 one has $G_{\min}(\boldsymbol{\rho}) = (|\mathcal{M}| + 1 + x_{\boldsymbol{\rho}})/2$, where

$$x_{\boldsymbol{\rho}} := \min_{\boldsymbol{\pi}\in\mathcal{P}(\mathcal{N}_{\mathcal{M}})} \sum_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right) \frac{\boldsymbol{\pi}\left(\mathbf{n}\right) - \boldsymbol{\pi}\left(\overline{\mathbf{n}}\right)}{2}\right].$$

Since for any $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}})$ the sum is lower bounded by its minimum term, one has

$$x_{\boldsymbol{\rho}} \geq y_{\boldsymbol{\rho}} := \min_{\substack{\boldsymbol{\pi}\in\mathcal{P}(\mathcal{N}(\mathcal{M})) \\ \mathbf{n}\in\mathcal{N}_{\mathcal{M}}}} \mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right) \frac{\boldsymbol{\pi}\left(\mathbf{n}\right) - \boldsymbol{\pi}\left(\overline{\mathbf{n}}\right)}{2}\right].$$

Using Lemma 2, for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ the minimum over $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}})$ can be computed leading to

$$y_{\boldsymbol{\rho}} = -\max_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \left\|E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\right\|_1.$$

Using Eq. (3), Lemma 3, and again $E_{\boldsymbol{\rho}}(\mathbf{n}) = -E_{\boldsymbol{\rho}}(\overline{\mathbf{n}})$, the maximum over $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ can be computed leading to

$$y_{\boldsymbol{\rho}} = -\left\|E_{\boldsymbol{\rho}}\left(\mathbf{n}^*\right)\right\|_1.$$

Since $G(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}) = (|\mathcal{M}|+1+y_{\boldsymbol{\rho}})/2$, the statement follows. □

The following corollary provides the analytical solution of the minimum guesswork problem for any qubit ensemble with uniform probability distribution.

Corollary 1: For any finite set $\mathcal{M}$, any two dimensional Hilbert space $\mathcal{H}$, and any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$ such that the prior probability distribution $\mathrm{Tr}[\boldsymbol{\rho}(\cdot)] = |\mathcal{M}|^{-1}$ is uniform, there exists numbering $\mathbf{n}^* \in \mathcal{N}_{\mathcal{M}}$ such that measurement $\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}$ minimizes the guesswork, that is

$$G_{\min}\left(\boldsymbol{\rho}\right) = G\left(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\right).$$

We remark that Corollary 1 recasts the minimum guesswork problem, by definition an optimization problem over a *continuous* set, as an optimization problem over a *finite* set, that can be therefore performed by exhaustive search.

Proof: Since by hypothesis $\mathrm{Tr}[\boldsymbol{\rho}(\cdot)] = |\mathcal{M}|^{-1}$, one has

$$\mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\right] = 0,$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Hence, since by hypothesis $\mathcal{H}$ is two-dimensional, one has

$$|E_{\boldsymbol{\rho}}(\mathbf{n})| = \|E_{\boldsymbol{\rho}}(\mathbf{n})\|_1 \frac{\mathbb{1}}{2},$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Hence, the range $|E_{\boldsymbol{\rho}}(\mathcal{N}(\mathcal{M}))|$ is totally ordered. Hence, there exists $\mathbf{n}^*$ such that

$$|E_{\boldsymbol{\rho}}(\mathbf{n}^*)| \geq |E_{\boldsymbol{\rho}}(\mathbf{n})| \geq E_{\boldsymbol{\rho}}(\mathbf{n}),$$

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Hence the statement follows from Theorem 1. □

IV. Explicit Examples

In this section we provide the minimum guesswork of any qubit regular polygonal or polyhedral ensemble by explicitly solving the optimization over a finite set given by Corollary 1.

Corollary 2 (Regular Polygonal Ensembles): For any discrete set $\mathcal{M}$, any two-dimensional Hilbert space $\mathcal{H}$, and any bijective ensemble $\boldsymbol{\rho} \in \mathbb{M}(\mathcal{M}, \mathcal{H})$ whose range $\boldsymbol{\rho}(\mathcal{M})$ is proportional to a regular polygon in the Bloch circle, one has

$$G_{\min}(\boldsymbol{\rho}) = \frac{|\mathcal{M}|+1}{2} - \frac{1}{2} \begin{cases} \frac{2\sqrt{3\cos\left(\frac{\pi}{|\mathcal{M}|}\right)^2+1}}{|\mathcal{M}|\sin\left(\frac{\pi}{|\mathcal{M}|}\right)^2}, & \text{if } |\mathcal{M}| \text{ even}, \\ \frac{\cos\left(\frac{\pi}{2|\mathcal{M}|}\right)}{|\mathcal{M}|\sin\left(\frac{\pi}{2|\mathcal{M}|}\right)^2}, & \text{if } |\mathcal{M}| \text{ odd}. \end{cases}$$

Proof: Due to Corollary 1, there exists numbering $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ such that $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho}, \boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$. Due to Lemma 4, $q_{\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}}$ is not increasing. One way of representing $\mathbf{n}^*$ is as follows. Without loss of generality take $\mathcal{M} = \{1, \ldots, |\mathcal{M}|\}$ and $\boldsymbol{\rho}(m) = |\mathcal{M}|^{-1} |\psi_m\rangle\langle\psi_m|$, where $|\psi_m\rangle = \cos(2\pi m/|\mathcal{M}|)\,|0\rangle + \sin(2\pi m/|\mathcal{M}|)\,|1\rangle$. Then one has

$$\mathbf{n}^*(m) = \begin{cases} 2\,m & \text{if } m < \frac{|\mathcal{M}|}{2} + \frac{1}{4}, \\ -2m + 2\,|\mathcal{M}| + 1 & \text{otherwise.} \end{cases}$$

Numbering $\mathbf{n}^*$ is illustrated in Fig. 1 for $|\mathcal{M}| = 8$. By summing finite trigonometric series, for $|\mathcal{M}|$ even one has

$$E_{\boldsymbol{\rho}}(\mathbf{n}^*) = \frac{1}{|\mathcal{M}|} \begin{bmatrix} -2\cot\left(\frac{\pi}{|\mathcal{M}|}\right)^2 - 1 & -\cot\left(\frac{\pi}{|\mathcal{M}|}\right) \\ -\cot\left(\frac{\pi}{|\mathcal{M}|}\right) & 2\cot\left(\frac{\pi}{|\mathcal{M}|}\right)^2 + 1 \end{bmatrix},$$

and for $|\mathcal{M}|$ odd one has

$$E_{\boldsymbol{\rho}}(\mathbf{n}^*) = \frac{1}{2\,|\mathcal{M}|} \begin{bmatrix} -\cot\left(\frac{\pi}{2|\mathcal{M}|}\right)^2 & -\cot\left(\frac{\pi}{2|\mathcal{M}|}\right) \\ -\cot\left(\frac{\pi}{2|\mathcal{M}|}\right) & \cot\left(\frac{\pi}{2|\mathcal{M}|}\right)^2 \end{bmatrix}.$$

By explicit computation one has

$$\|E_{\boldsymbol{\rho}}(\mathbf{n}^*)\|_1 = \begin{cases} 2\frac{\sqrt{3\cos\left(\frac{\pi}{|\mathcal{M}|}\right)^2+1}}{|\mathcal{M}|\sin\left(\frac{\pi}{|\mathcal{M}|}\right)^2}, & \text{if } |\mathcal{M}| \text{ even}, \\ \frac{\cos\left(\frac{\pi}{2|\mathcal{M}|}\right)}{|\mathcal{M}|\sin\left(\frac{\pi}{2|\mathcal{M}|}\right)^2}, & \text{if } |\mathcal{M}| \text{ odd}. \end{cases}$$

Hence the statement follows from Eq. (2). □

Corollary 3 (Regular Polyhedral Ensembles): For any discrete set $\mathcal{M}$, any two-dimensional Hilbert space $\mathcal{H}$, and any bijective ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M}, \mathcal{H})$ whose range $\boldsymbol{\rho}(\mathcal{M})$ is proportional to a regular polyhedron in the Bloch sphere, one has

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

Proof: Due to Corollary 1, there exists numbering $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ such that $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho}, \boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$. For $|\mathcal{M}| = 4$ any $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ is such that $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho}, \boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$, hence the

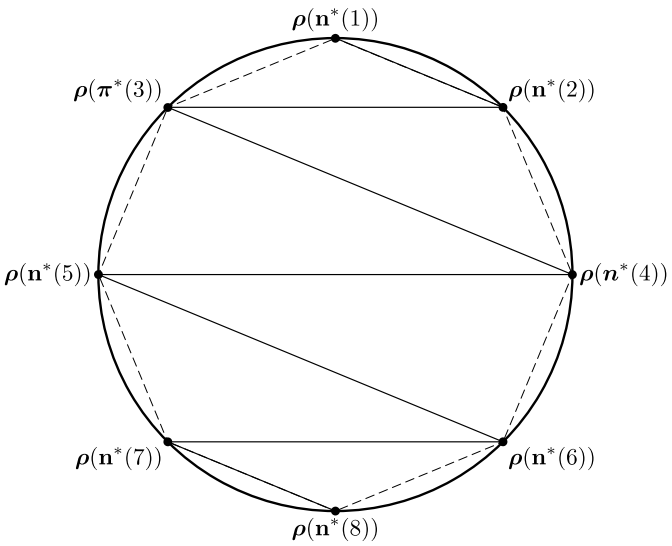

Fig. 1. The figure illustrates the numbering $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ such that $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho}, \boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$, when $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M}, \mathbb{R}^2)$ is a bijective ensemble such that $\boldsymbol{\rho}(\mathcal{M})$ is proportional to a regular polygon ($|\mathcal{M}| = 8$ in the figure) in the Bloch circle.

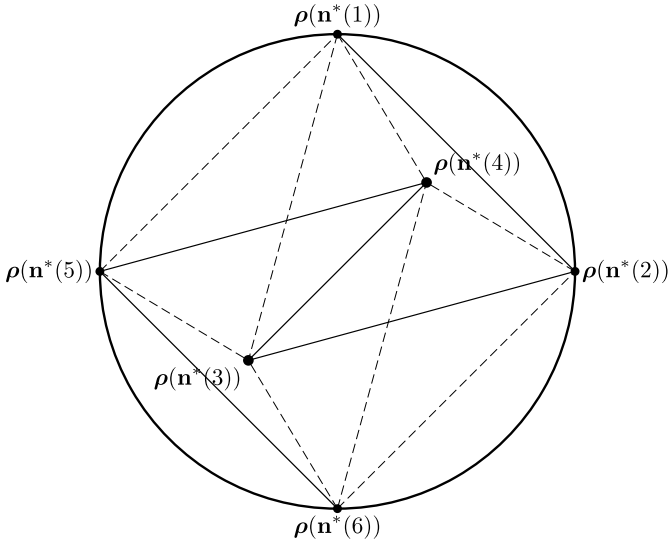

Fig. 2. The figure illustrates the numbering $\mathbf{n}^* \in \mathcal{N}(\mathcal{M})$ such that $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho}, \boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$, when $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M}, \mathbb{C}^2)$ is a bijective ensemble such that $\boldsymbol{\rho}(\mathcal{M})$ is proportional to a regular polyhedron ($|\mathcal{M}| = 6$ in the figure) in the Bloch sphere.

result for $|\mathcal{M}| = 4$ follows. Let us consider the case $|\mathcal{M}| > 4$. Due to Lemma 4, $q_{\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}}$ is not increasing. Since the range $\boldsymbol{\rho}(\mathcal{M})$ is centrally symmetric, that is

$$\boldsymbol{\rho}\left(\mathcal{M}\right) = \left|\mathcal{M}\right|^{-1} \mathbb{1} - \boldsymbol{\rho}\left(\mathcal{M}\right),$$

any $\mathbf{n}^*$ with $q_{\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}}$ not increasing satisfies

$$\boldsymbol{\rho}\left(\mathbf{n}^*\left(\cdot\right)\right) + \boldsymbol{\rho}\left(\overline{\mathbf{n}}^*\left(\cdot\right)\right) = \left|\mathcal{M}\right|^{-1} \mathbb{1}.$$

Since fixing the value of $\mathbf{n}^*(t)$ also fixes the value of $\overline{\mathbf{n}}^*(t)$, numbering $\mathbf{n}^*$ can be found in $|\mathcal{M}|!!$ steps. Also, since regular polyhedra are vertex transitive, the choice of $\mathbf{n}^*(1)$ is irrelevant, hence $\mathbf{n}^*$ can be found in $|\mathcal{M}-2|!!$ steps. The exhaustive search is practical even for the dodecahedron for which $|\mathcal{M}| = 20$ and hence $|\mathcal{M}-2|!! \sim 10^8$. Numbering $\mathbf{n}^*$ is illustrated in Fig. 2 for $|\mathcal{M}| = 6$. Hence the results for $|\mathcal{M}| > 4$ follow. Further details can be found in Ref. [15], where algorithms for the classical computation of the quantum guesswork in analytical closed form based on the present results are provided and analyzed. □

APPENDIX

In this appendix we derive technical results needed for the derivation of our main results.

Lemma 1: For any finite set $\mathcal{M}$, any finite dimensional Hilbert space $\mathcal{H}$, any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, and any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$, the guesswork $G(\boldsymbol{\rho},\boldsymbol{\pi})$ is given by

$$G\left(\boldsymbol{\rho},\boldsymbol{\pi}\right) = \frac{\left|\mathcal{M}\right|+1}{2} + \frac{1}{2}\sum_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\frac{\boldsymbol{\pi}\left(\mathbf{n}\right)-\boldsymbol{\pi}\left(\overline{\mathbf{n}}\right)}{2}\right].$$

Proof: By definition of map $E_{\boldsymbol{\rho}}$ one has $G(\boldsymbol{\rho},\boldsymbol{\pi}) = (|\mathcal{M}|+1+x_{\boldsymbol{\rho},\boldsymbol{\pi}})/2$, where

$$x_{\boldsymbol{\rho},\boldsymbol{\pi}} := \sum_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\boldsymbol{\pi}\left(\mathbf{n}\right)\right].$$

Using the identity $E_{\boldsymbol{\rho}}(\mathbf{n}) = -E_{\boldsymbol{\rho}}(\overline{\mathbf{n}})$ one has

$$x_{\boldsymbol{\rho},\boldsymbol{\pi}} = \sum_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \mathrm{Tr}\left[E_{\boldsymbol{\rho}}\left(\mathbf{n}\right)\frac{\boldsymbol{\pi}\left(\mathbf{n}\right)-\boldsymbol{\pi}\left(\overline{\mathbf{n}}\right)}{2}\right].$$

Hence the statement follows. □

For any finite dimensional Hilbert space $\mathcal{H}$ and any operator $A \in \mathcal{L}(\mathcal{H})$, let $\mathcal{P}_A : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ be a dephasing map given by $\mathcal{P}_A(\cdot) = \sum_a \langle a|\cdot|a\rangle\,|a\rangle\langle a|$, where $\{|a\rangle\}$ is a complete set of eigenvectors of A.

Lemma 2: For any finite dimensional Hilbert space $\mathcal{H}$ and any $X, A \in \mathcal{L}(\mathcal{H})$, if $|X| \leq \mathbb{1}$ one has that $|\,\mathrm{Tr}[AX]| \leq \|A\|_1$.

Proof: Since $\mathcal{P}_A$ is linear, positive, and unital, by the hypothesis it follows that $|\mathcal{P}_A(X)| \leq \mathbb{1}$. Since $\mathrm{Tr}[AX] = \mathrm{Tr}[A\mathcal{P}_A(X)]$, the statement follows. □

Lemma 3: For any finite dimensional Hilbert space $\mathcal{H}$ and any $X, A \in \mathcal{L}(\mathcal{H})$, if $-X \leq A \leq X$ one has that $\|A\|_1 \leq \|X\|_1$.

Proof: Since $\mathcal{P}_A$ is linear and positive and $\mathcal{P}_A(A) = A$, by the hypothesis it follows that $-\mathcal{P}_A(X) \leq A \leq \mathcal{P}_A(X)$. Since $[\mathcal{P}_A(X), A] = 0$ and by the hypothesis it follows that $X \geq 0$, one has $|A| \leq \mathcal{P}_A(X)$. Since $\mathcal{P}_A$ is trace preserving, by tracing both sides the statement follows. □

The following lemma provides a necessary condition for any measurement to attain the minimum guesswork.

Lemma 4: For any discrete set $\mathcal{M}$, any finite dimensional Hilbert space $\mathcal{H}$, and any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, a measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$ minimizes the guesswork, that is $G_{\min}(\boldsymbol{\rho}) = G(\boldsymbol{\rho},\boldsymbol{\pi})$, 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 measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$ there exists a measurement $\boldsymbol{\pi}' \in \mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$ such that $p_{\boldsymbol{\rho},\boldsymbol{\pi}'}(\mathbf{n},\cdot)$ is not increasing for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ and $G(\boldsymbol{\rho},\boldsymbol{\pi}') \leq G(\boldsymbol{\rho},\boldsymbol{\pi})$, with equality if and only if $p_{\boldsymbol{\rho},\boldsymbol{\pi}}(\mathbf{n},\cdot) = p_{\boldsymbol{\rho},\boldsymbol{\pi}'}(\mathbf{n},\cdot)$ for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Let $\{g_{\mathbf{n}} : \{1,\ldots,|\mathcal{M}|\} \to \{1,\ldots,|\mathcal{M}|\} \mid g_{\mathbf{n}} \text{ bijective}\}_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}}$ be a family of permutations such that $p_{\boldsymbol{\rho},\boldsymbol{\pi}}(\mathbf{n}, g_{\mathbf{n}}(\cdot))$ is not increasing for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. Let $f : \mathcal{N}_{\mathcal{M}} \to \mathcal{N}_{\mathcal{M}}$ be given by

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

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

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

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

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

for any $t \in \{1,\ldots,|\mathcal{M}|\}$. Hence by construction

$$\sum_{t\in\{1,\ldots,T\}} q_{\boldsymbol{\rho},\boldsymbol{\pi}'}\left(t\right) \geq \sum_{t\in\{1,\ldots,T\}} q_{\boldsymbol{\rho},\boldsymbol{\pi}}(t)$$

for any $T \in \{1,\ldots,|\mathcal{M}|\}$, with equality if and only if $p_{\boldsymbol{\rho},\boldsymbol{\pi}}(\mathbf{n},\cdot) = p_{\boldsymbol{\rho},\boldsymbol{\pi}'}(\mathbf{n},\cdot)$ for any $\mathbf{n} \in \mathcal{N}(\mathcal{M})$. Hence the statement follows by definition of guesswork. □

V. CONCLUSION

The guesswork of a quantum ensemble quantifies the minimum number of guesses needed in average to correctly guess the state of the ensemble, when only one state can be queried at a time. Here, we derived analytical solutions subject to a finite set of conditions, including analytical solutions for any qubit ensemble with uniform probability distribution, thus disproving the conjecture [13] that analytical solutions only exist for binary and symmetric ensembles. As explicit examples, we computed the guesswork for any qubit regular polygonal and polyhedral ensemble, thus proving a conjecture [14] on the guesswork of the square qubit ensemble.

ACKNOWLEDGMENT

Michele Dall'Arno is grateful to Eric Hanson and Nilanjana Datta for insightful discussions during a visit to the University of Cambridge.

REFERENCES

[1] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[2] J. Massey, "Guessing and entropy," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 1994, p. 204.

[3] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 99–105, Jan. 1996.

[4] E. Arikan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inf. Theory* vol. 44, no. 1, pp. 99–105, Jan. 1996.

[5] E. Arikan and N. Merhav, "Joint source-channel coding and guessing with application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1756–1769, Sep. 1998.

[6] J. Pliam, "The disparity between work and entropy in cryptology," in *Proc. IACR*, 1998, pp. 1–16.

[7] D. Malone and W. Sullivan, "Guesswork and entropy," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 525–526, Mar. 2004.

[8] R. Sundaresan, "Guessing under source uncertainty," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 269–287, Jan. 2007.

[9] M. K. Hanawal and R. Sundaresan, "Guessing revisited: A large deviations approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 70–78, Jan. 2011.

[10] M. M. Christiansen and K. R. Duffy, "Guesswork, large deviations, and Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 796–802, Feb. 2013.

[11] I. Sason and S. Verd, "Improved bounds on lossless source coding and guessing moments via Rényi measures," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4323–4346, Jun. 2018.

[12] I. Sason, "Tight bounds on the Rényi entropy via majorization with applications to guessing and compression," *Entropy*, vol. 20, p. 896, Apr. 2018.

[13] W. Chen, Y. Cao, H. Wang, and Y. Feng, "Minimum guesswork discrimination between quantum states," *Quantum Inf. Comput.*, vol. 15, p. 0737, Apr. 2015.

[14] E. P. Hanson, V. Katariya, N. Datta, and M. M. Wilde, "Guesswork with quantum side information," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 322–338, Jan. 2022.

[15] M. Dall'Arno, F. Buscemi, and T. Koshiba, "Classical computation of quantum guesswork," 2021, *arXiv:2112.01666*.

Michele Dall'Arno received the Ph.D. degree in theoretical physics from the University of Pavia, Italy, in 2012. He held post-doctoral positions at ICFO, Barcelona, Nagoya University, Japan, and the National University of Singapore. Since 2020, he has been an Assistant Professor in quantum information with Kyoto University and a Visiting Researcher with Waseda University, Tokyo.

Francesco Buscemi received the Ph.D. degree in theoretical physics from the University of Pavia, Italy, in 2006. After post-doctoral positions in Tokyo, Japan, and Cambridge, U.K., he joined Nagoya University in 2009, where he is currently a Professor with the Department of Mathematical Informatics. In 2018, he was awarded the Birkhoff-von Neumann Prize by the International Quantum Structures Association.

Takeshi Koshiba (Member, IEEE) received the Ph.D. degree from the Tokyo Institute of Technology, Tokyo, Japan. He is currently a Full Professor at the Department of Mathematics, Faculty of Education and Integrated Arts and Sciences, Waseda University, Tokyo. His research interests include theoretical and applied cryptography, randomness in algorithms, and quantum computing, cryptography, and information.