Guesswork of a Quantum Ensemble

Based on arXiv:2012.09350

Michele Dall'Arno (Kyoto University and Waseda University, Japan)
Francesco Buscemi (Nagoya University, Japan)
Takeshi Koshiba (Waseda University, Japan)

QICF21
September 17, 2021

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.

We derive **analytical solutions** subject to a **finite set of conditions**, including analytical solutions for any **qubit ensemble** with **uniform probability distribution**.

As explicit examples, we compute the guesswork for any qubit regular polygonal and polyhedral ensemble.

A communication scenario involving Alice and Bob

Data: an ensemble ρ of quantum states with labels in a set $\mathcal{M}$ known to both parties.

At each round:

1. Alice picks a label $m \in \mathcal{M}$ with probability $\mathrm{Tr}[\rho(m)]$ and hands state $\mathrm{Tr}[\rho(m)]^{-1}\rho(m)$ over to Bob;
2. 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.

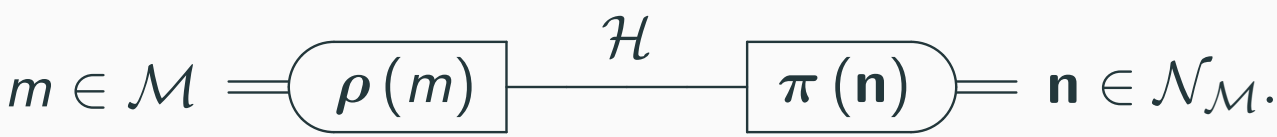
Cost function incurred by Bob: the average number of guesses, or *guesswork*, until he correctly guesses m.

Bob's most general strategy

Bob's **most general strategy** consists of performing a quantum measurement π 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 $\mathbf{n}$.

The guesswork is given by the occurence of label m in numbering $\mathbf{n}$, averaged over all numberings.

The setup is as follows:



Guesswork extensively studied in the classical case

1. J. Massey, Proceedings of 1994 IEEE International Symposium on Information Theory, 204 (1994).
2. E. Arikan, IEEE Trans. Inform. Theory **42**, 99 (1996).
3. E. Arikan and N. Merhav, IEEE Trans. Inform. Theory **44**, 1041 (1998).
4. E. Arikan and N. Merhav, IEEE Trans. Inform. Theory **44**, 1756 (1998).
5. D. Malone and W. Sullivan, IEEE Trans. Inform. Theory **50**, 525 (2004).
6. R. Sundaresan, IEEE Trans. Inform. Theory **53**, 269 (2007).
7. M. K. Hanawal and R. Sundaresan, arXiv:1008.1977.
8. M. M. Christiansen and K. R. Duffy, IEEE Trans. Inform. Theory **59**, 796 (2013).
9. I. Sason and S. Verdú, arXiv:1801.01265.
10. I. Sason, Entropy **20**, 896 (2018).

Not much is known in the quantum case

Only two works (AFAIK) on quantum guesswork, focusing on entropic bounds without providing analytical solutions:

1. W. Chen, Y. Cao, H. Wang, and Y. Feng, Quantum Information & Computation **15**, 0737 (2015).

   [While discussing quantum state discrimination] "Closed-form result or optimal measurement is only known for some special quantum systems, e.g., the case with exactly two states, equiprobable symmetric states, or multiply symmetric states. We believe that it is also the case for minimum guesswork discrimination, because of the analogy between these two problems."

2. E. P. Hanson, V. Katariya, N. Datta, and M. M. Wilde, arXiv:2001.03598. Conjecture on the guesswork of the square ensemble.

Our results (disproving former belief)

Main result : analytical solution subject to a *finite* set of conditions.

Corollary : analytical solution for any qubit ensemble with uniform probability distribution, thus disproving Conjecture [Chen, Cao, Wang, Feng, 2015].

Explicit examples : guesswork of any qubit regular polygonal and polyhedral ensebles, respectively, thus proving Conjecture [Hanson, Katariya, Datta, Wilde, 2020].

Sets of ensembles and numbering-valued measurements

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

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

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

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

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

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

Probability distributions

For any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M}, \mathcal{H})$ and any numbering-valued measurement $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}}, \mathcal{H})\boldsymbol{\rho}$, 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:

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

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:

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

Guesswork of a quantum ensemble

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

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

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

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

A map that makes explicit the symmetries of the problem

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

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

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

For any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, let $\overline{\mathbf{n}}$ be the **reversed numbering**:

$$\overline{\mathbf{n}}(t) := \mathbf{n}(|\mathcal{M}| + 1 - t), \qquad \forall t \in \{1, \ldots, |\mathcal{M}|\}.$$

Map $E_{\boldsymbol{\rho}}$ has the following simple symmetry, among others:

$$E_{\boldsymbol{\rho}}(\mathbf{n}) = -E_{\boldsymbol{\rho}}(\overline{\mathbf{n}}), \qquad \forall \mathbf{n} \in \mathcal{N}_{\mathcal{M}}.$$

A family of tests (candidate for optimality)

Let $\{\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}})\}_{\mathbf{n}^* \in \mathcal{N}_{\mathcal{M}}}$ be the family of **numbering-valued measurements** given by

$$\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}(\mathbf{n}) := \begin{cases} \left(\Pi_- + \frac{1}{2}\Pi_0\right)\left(E_{\boldsymbol{\rho}}(\mathbf{n})\right), & \text{if } \mathbf{n} \in \{\mathbf{n}^*, \overline{\mathbf{n}}^*\}, \\ 0, & \text{otherwise}, \end{cases}$$

for any $\mathbf{n}^*, \mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, where $\Pi_-(\cdot)$ and $\Pi_0(\cdot)$ are the projectors on the negative and null parts of $(\cdot)$, respectively.

By using the identity $E_{\boldsymbol{\rho}}(\mathbf{n}) = -E_{\boldsymbol{\rho}}(\overline{\mathbf{n}})$ for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, the corresponding guesswork can be computed leading to

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

Main result

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

$$|E_{\boldsymbol{\rho}}(\mathbf{n}^*)| \geq E_{\boldsymbol{\rho}}(\mathbf{n}), \tag{1}$$

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

Remark: while the minimum guesswork problem is by definition an optimization over a *continuous* set, the conditions given by Eq. (1) are *finite* in number and hence can be checked by exhaustive search.

Sketch of the proof of the theorem

By using the identity $E_{\boldsymbol{\rho}}(\mathbf{n}) = -E_{\boldsymbol{\rho}}(\overline{\mathbf{n}})$ for any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, one has $G_{\min}(\boldsymbol{\rho}) = (|\mathcal{M}| + 1 + x_{\boldsymbol{\rho}})/2$, where

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

Since the sum is lower bounded by its minimum term, one has

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

For any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ the minimum over $\boldsymbol{\pi} \in \mathcal{P}(\mathcal{N}_{\mathcal{M}})$ is given by

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

The minimum over $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$ is given by

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

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

Qubit ensembles satisfy the hypothesis of the theorem

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

Remark: the corollary 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 of the corollary

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

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

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

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

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

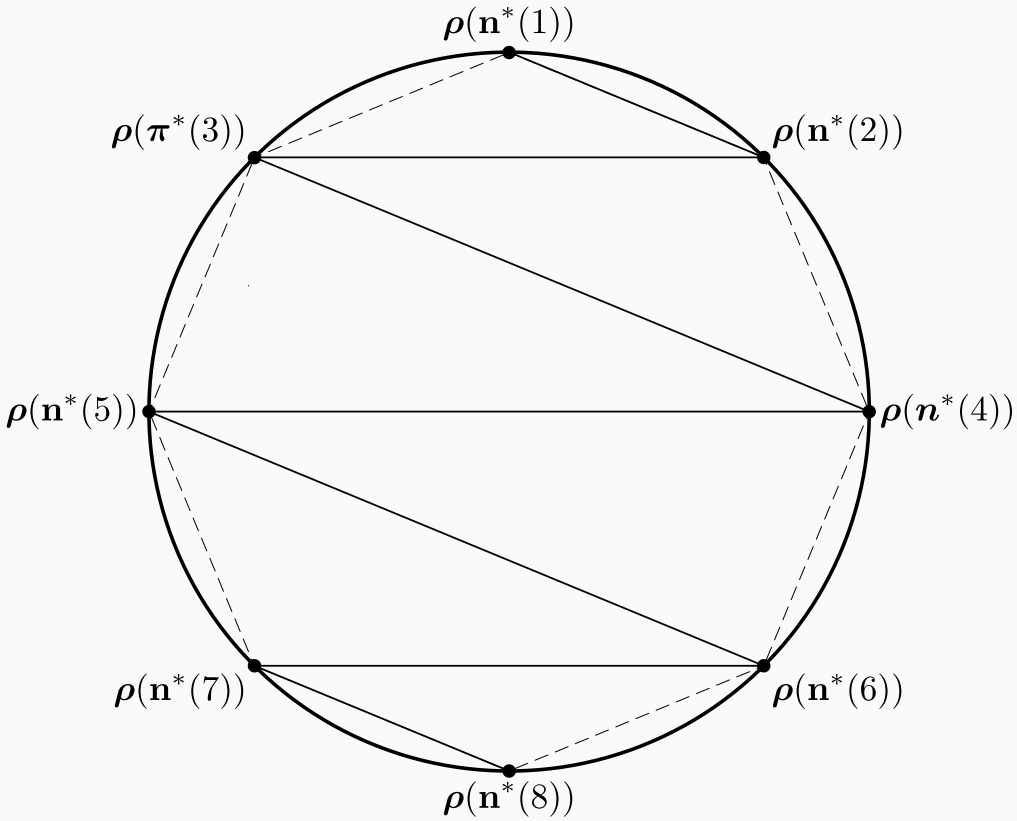
Guesswork of regular polygonal ensembles

The following corollary provides the minimum guesswork of any qubit regular polygonal ensemble by explicitly solving the aforementioned optimization over a finite set.

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

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

Optimal numbering for regular polygonal ensembles



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.

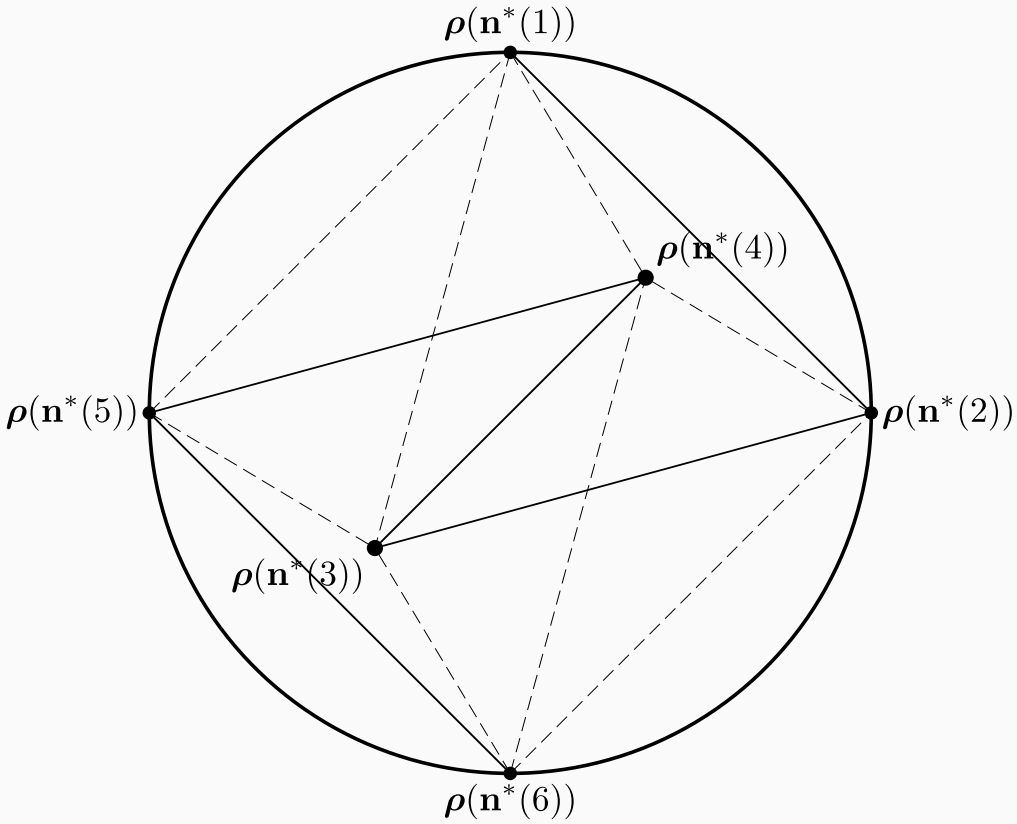
Guesswork of regular polyhedral ensembles

The following corollary provides the minimum guesswork of any qubit regular polyhedral ensemble by explicitly solving the aforementioned optimization over a finite set.

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

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

Optimal numbering for regular polyhedral ensembles



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.

Conclusion, and thank you for your attention!

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.

We derived analytical solutions subject to a finite set of conditions, including analytical solutions for any qubit ensemble with uniform probability distribution, thus disproving Conjecture [Chen, Cao, Wang, Feng, 2015] 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 Conjecture [Hanson, Katariya, Datta, Wilde, 2020] on the guesswork of the square qubit ensemble.

Further details can be found in [arXiv:2012.09350].