Quantum guesswork: a combinatorial instance of quantum hypothesis testing

Michele Dall'Arno

Department of Computer Science and Engineering, Toyohashi University of Technology, Japan

Operational setup

The guesswork problem can be conveniently framed as a theoretical game involving two parties, say Alice and Bob. At each round, Alice and Bob are given a classical and a quantum state, respectively, the latter solely dependant on the former. Bob queries Alice one state at a time until he correctly guesses her classical state, at which point he pays a cost that solely depends on the number of queries he had to perform. The probability distribution according to which classical states are sampled, the mapping between classical and quantum states, as well as the cost function, are known in advance to the parties. The minimum guesswork problem consists of the minimization of Bob's average cost.

Formalization

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

For any finite set $\mathcal{M}$ and any finite-dimensional Hilbert space $\mathcal{H}$, we denote with $\mathcal{E}(\mathcal{M},\mathcal{H})$ the set of ensembles from $\mathcal{M}$ to $\mathcal{H}$ given by

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

For any finite set $\mathcal{M}$, we denote with $\mathcal{N}_{\mathcal{M}}$ the set of numberings of $\mathcal{M}$ given by

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

For any finite set $\mathcal{M}$ and any Hilbert space $\mathcal{H}$, we denote with $\mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H})$ the set of numbering-valued measurements given by

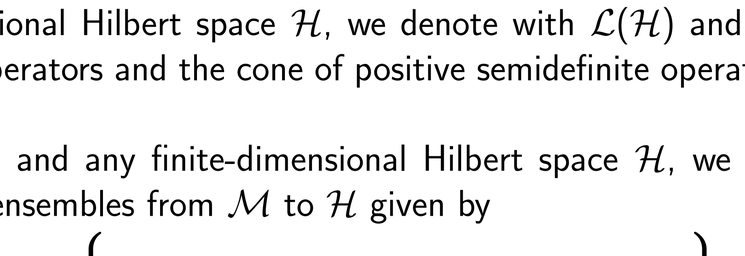
$$\mathcal{P}\left(\mathcal{N}_{\mathcal{M}},\mathcal{H}\right) := \left\{ \boldsymbol{\pi} : \mathcal{N}_{\mathcal{M}} \to \mathcal{L}_+\left(\mathcal{H}\right) \,\middle|\, \sum_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \boldsymbol{\pi}\left(\mathbf{n}\right) = \mathbb{1} \right\}.$$

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

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

or, in the quantum circuit formalism,

$$p_{\boldsymbol{\rho},\boldsymbol{\pi}}\left(\mathbf{n},t\right) =$$



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

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

For any finite set $\mathcal{M}$, any function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, and any finite dimensional Hilbert space $\mathcal{H}$, we denote with G^{γ} the *guesswork* function with single-measurement strategy, that is, the expectation value of γ given by

$$\begin{aligned} G^{\gamma} &: \mathcal{E}\left(\mathcal{M},\mathcal{H}\right) \times \mathcal{P}\left(\mathcal{N}_{\mathcal{M}},\mathcal{H}\right) \to \mathbb{R} \\ &(\boldsymbol{\rho},\boldsymbol{\pi}) \mapsto \sum_{t=1}^{|\mathcal{M}|} \gamma\left(t\right) q_{\boldsymbol{\rho},\boldsymbol{\pi}}\left(t\right). \end{aligned}$$

Definition (Minimum guesswork)

For any finite set $\mathcal{M}$, any function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, any finite dimensional Hilbert space $\mathcal{H}$, and any ensemble $\boldsymbol{\rho}(\mathcal{M},\mathcal{H})$ the minimum guesswork $G^{\gamma}_{\mathrm{min}}$ is given by

$$G^{\gamma}_{\mathrm{min}}\left(\boldsymbol{\rho}\right) = \min_{\boldsymbol{\pi}\in\mathcal{P}(\mathcal{N}_{\mathcal{M}},\mathcal{H}_0)} G^{\gamma}\left(\boldsymbol{\rho},\boldsymbol{\pi}\right).$$

Main result

For any discrete function f, we denote with $\overline{f}$ its average. For any finite set $\mathcal{M}$, any function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, any finite-dimensional Hilbert space $\mathcal{H}$, and any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, we denote with $E^{\gamma}_{\boldsymbol{\rho}} : \mathcal{N}_{\mathcal{M}} \to \mathcal{L}(\mathcal{H})$ the map given by

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

for any $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$. We say that function γ is balanced if and only if there exists permutation σ_{γ} such that

$$\frac{\gamma + \gamma\circ\sigma_{\gamma}^{-1}}{2} = \overline{\gamma}.$$

We denote with $\Pi_{-}(\cdot)$ and $\Pi_{0}(\cdot)$ the projectors on the negative and null parts of $(\cdot)$, respectively. For any finite set $\mathcal{M}$, any balanced function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, any finite-dimensional Hilbert space $\mathcal{H}$, any ensemble $\boldsymbol{\rho} \in \mathcal{E}(\mathcal{M},\mathcal{H})$, and any $\mathbf{n}^* \in \mathcal{N}_{\mathcal{M}}$, we denote with $\boldsymbol{\pi}^{\gamma}_{\boldsymbol{\rho},\mathbf{n}^*}$ the numbering-valued measurement given by

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

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

Theorem (Closed-form guesswork under a finite set of conditions)

For any finite set $\mathcal{M}$, any balanced function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, 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

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

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 $G^{\gamma}_{\mathrm{min}}(\boldsymbol{\rho}) = G^{\gamma}(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*})$, with

$$G^{\gamma}\left(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\right) = \overline{\gamma} - \frac{1}{2}\left\|E^{\gamma}_{\boldsymbol{\rho}}\left(\mathbf{n}^*\right)\right\|_1.$$

The qubit case

For any function $f : \{1,\dots,M\} \to K$, where K is a linear space, we denote with $\mathrm{gram}(f)$ the Gram matrix whose element i,j is $f(i)\cdot f(j)$. For any set $\mathcal{M} = \{1,\dots,|\mathcal{M}|\}$ and any numbering $\mathbf{n} \in \mathcal{N}_{\mathcal{M}}$, we denote with $X_{\mathbf{n}}$ the $|\mathcal{M}|\times|\mathcal{M}|$ permutation matrix whose element i,j is $\delta_{i,\mathbf{n}(j)}$. For any two-dimensional Hilbert space $\mathcal{H}$, let $\mathbf{v}$ be the Pauli vector function given by

$$\begin{aligned} &\mathbf{v} : \mathcal{L}\left(\mathcal{H}\right) \to \mathbb{R}^3 \\ &A \mapsto \left(\mathrm{Tr}\left[A\sigma_k\right]\right)_{k=1}^{3}, \end{aligned}$$

for some orthonormal basis $(\sigma_k)_{k=1}^{3}$ in the traceless subspace of $\mathcal{L}(\mathcal{H})$ equipped with the Hilbert-Schmidt product.

Corollary (Guesswork of qubit ensembles)

For any set $\mathcal{M} = \{1,\dots,|\mathcal{M}|\}$, any balanced function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, 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, the measurement $\boldsymbol{\pi}^{\gamma}_{\boldsymbol{\rho},\mathbf{n}^*}$ attains the minimum guesswork $G^{\gamma}_{\mathrm{min}}(\boldsymbol{\rho})$, that is $G^{\gamma}_{\mathrm{min}}(\boldsymbol{\rho}) = G^{\gamma}(\boldsymbol{\rho},\boldsymbol{\pi}^{\gamma}_{\mathbf{n}^*})$, where $\mathbf{n}^*$ is the solution of the following quadratic assignment problem

$$\mathbf{n}^* = \arg\max_{\mathbf{n}\in\mathcal{N}_{\mathcal{M}}} \mathrm{Tr}\left[\mathrm{gram}\left(\gamma - \overline{\gamma}\right) X_{\mathbf{n}}\, \mathrm{gram}\left(\mathbf{v}\circ\boldsymbol{\rho}\right) X_{\mathbf{n}}^{T}\right],$$

and one has

$$G^{\gamma}\left(\boldsymbol{\rho},\boldsymbol{\pi}_{\boldsymbol{\rho},\mathbf{n}^*}\right) = \overline{\gamma} - \frac{1}{2}\left|\mathbf{v}\left(E^{\gamma}_{\boldsymbol{\rho}}\left(\mathbf{n}^*\right)\right)\right|_2.$$

A square matrix A is Toeplitz if and only if its entry $A_{i,j}$ only depends on $i-j$ for any i and j. A matrix A is benevolent if and only if it is symmetric, Toeplitz, and satisfies the following properties:

1. $A_{m+1,1}$ is a non-decreasing function of m in $\{1,\dots,\lfloor|\mathcal{M}|/2\rfloor\}$.
2. $A_{|\mathcal{M}|+1-m,1} \geq A_{m+1,1}$ for any $m \in \{1,\dots,\lfloor(|\mathcal{M}|/2\rfloor\}$.

For any set $\mathcal{M} = \{1,\dots,|\mathcal{M}|\}$ we define the numbering $\mathbf{n}_{\mathrm{bv}}$ given by

$$\left(\mathbf{n}_{\mathrm{bv}}\right)^{-1}\left(m\right) := \begin{cases} 2m-1 & \text{if } m \leq \lceil|\mathcal{M}/2\rceil, \\ 2\left(|\mathcal{M}|+1-m\right) & \text{otherwise.} \end{cases}$$

Corollary (Guesswork of benevolent ensembles)

For any set $\mathcal{M} = \{1,\dots,|\mathcal{M}|\}$, any balanced function $\gamma : \{1,\dots,|\mathcal{M}|\} \to \mathbb{R}$, 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, if $-\mathrm{gram}(\mathbf{v}\circ\boldsymbol{\rho})$ is permutationally equivalent to a benevolent matrix and $\mathbf{v}(\overline{\boldsymbol{\rho}})\cdot\mathbf{v}(\boldsymbol{\rho}(\cdot))$ is constant, the measurement $\boldsymbol{\pi}^{\gamma}_{\boldsymbol{\rho},\mathbf{n}^*}$ attains the minimum guesswork $G^{\gamma}_{\mathrm{min}}(\boldsymbol{\rho})$, that is $G^{\gamma}_{\mathrm{min}}(\boldsymbol{\rho}) = G^{\gamma}(\boldsymbol{\rho},\boldsymbol{\pi}^{\gamma}_{\boldsymbol{\rho},\mathbf{n}^*})$, where $\mathbf{n}^* = \sigma_2\circ\mathbf{n}_{\mathrm{bv}}\circ\sigma_1^{-1}$ and permutations σ_1,σ_2 are such that $\gamma\circ\sigma_1$ is non-decreasing and $-\mathrm{gram}(\mathbf{v}\circ\boldsymbol{\rho}\circ\sigma_2)$ is benevolent.

- M. Dall'Arno, F. Buscemi, and T. Koshiba, *Guesswork of a quantum ensemble*, IEEE Trans. Inform. Theory **68**, 3193 (2022).
- M. Dall'Arno, F. Buscemi, and T. Koshiba, *Classical computation of quantum guesswork*, arXiv:2112.01666.
- M. Dall'Arno, *Quantum guesswork*, arXiv:2302.06783.