Private and Robust States for Distributed Quantum Sensing

Luís Bugalho[1,2,3,4] Majid Hassani[4], Yasser Omar[1,2,3], and Damian Markham[4]

1 Instituto Superior Técnico, Universidade de Lisboa, Portugal
2 Physics of Information and Quantum Technologies Group, CeFEMA, Portugal
3 PQI – Portuguese Quantum Institute, Portugal
4 Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France

arXiv:2407.21701

Distributed Sensing

Distributed quantum sensing enables the estimation of multiple parameters encoded in spatially separated probes. While traditional quantum sensing is often focused on estimating a single parameter with maximum precision, distributed quantum sensing seeks to estimate some function of multiple parameters that are only locally accessible for each party involved. In such settings it is natural to not want to give away more information than is necessary - **privacy**. To do this, one should find which states comply with this - **private states**. Applications can range from clock synchronization protocols, to gravimetry experiments.

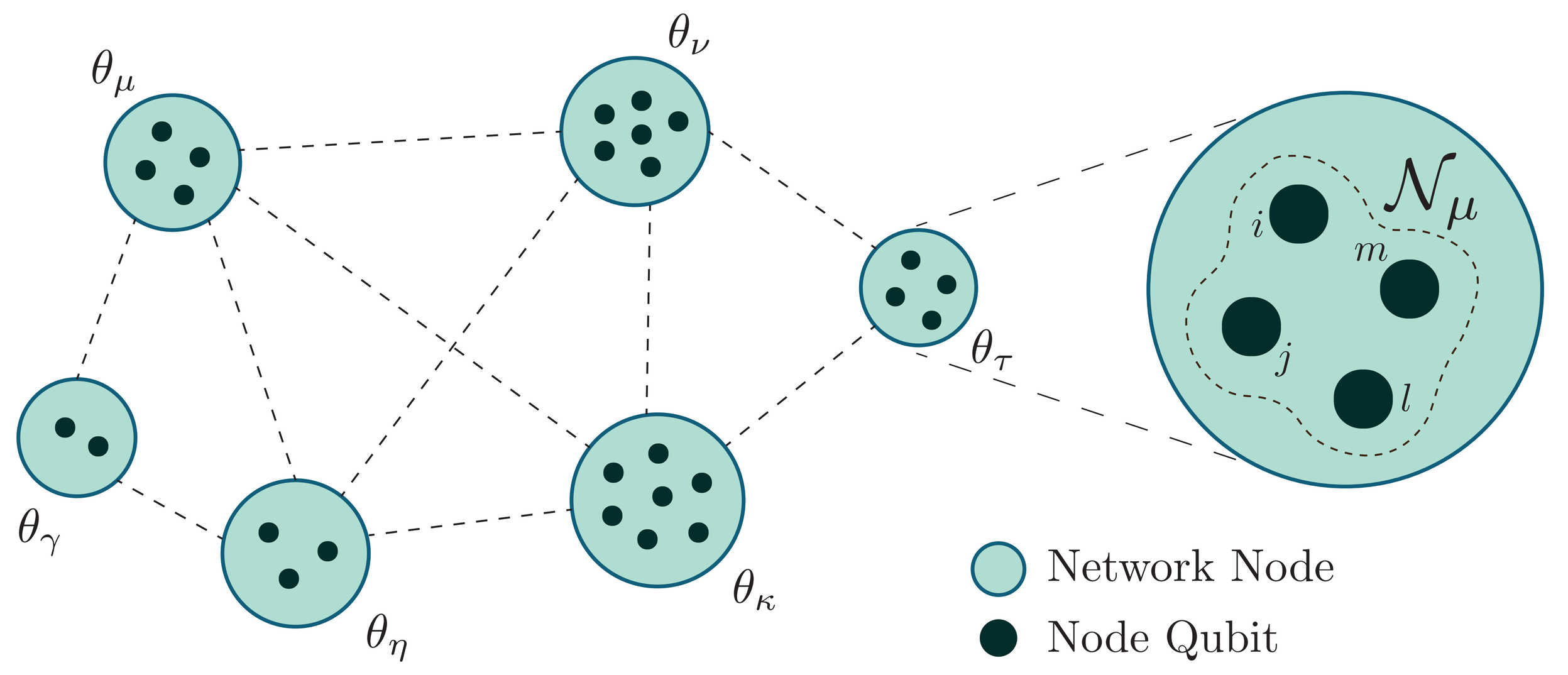


Figure 1. Distributed sensing scenario, consisting of a) a network of quantum nodes, capableof distributing entangled states, where b) each of the nodes holds their own sets of qubits, which can be seen as resources for quantum sensing.

Private Quantum Information

We start from building a target linear function of the distributed parameters:

$$f(\theta) = a \cdot \theta$$

The definition of privacy can be stated from the following conditions:
(i) Let H and D be the subsets of honest and dishonest parties;
(ii) Every honest party in H can only know the target function
(iii) Every dishonest party in D can only know the target function and all indidividual parameters in D (and any linear combination thereof).

Then one can define a privacy measure with respect to a target function:

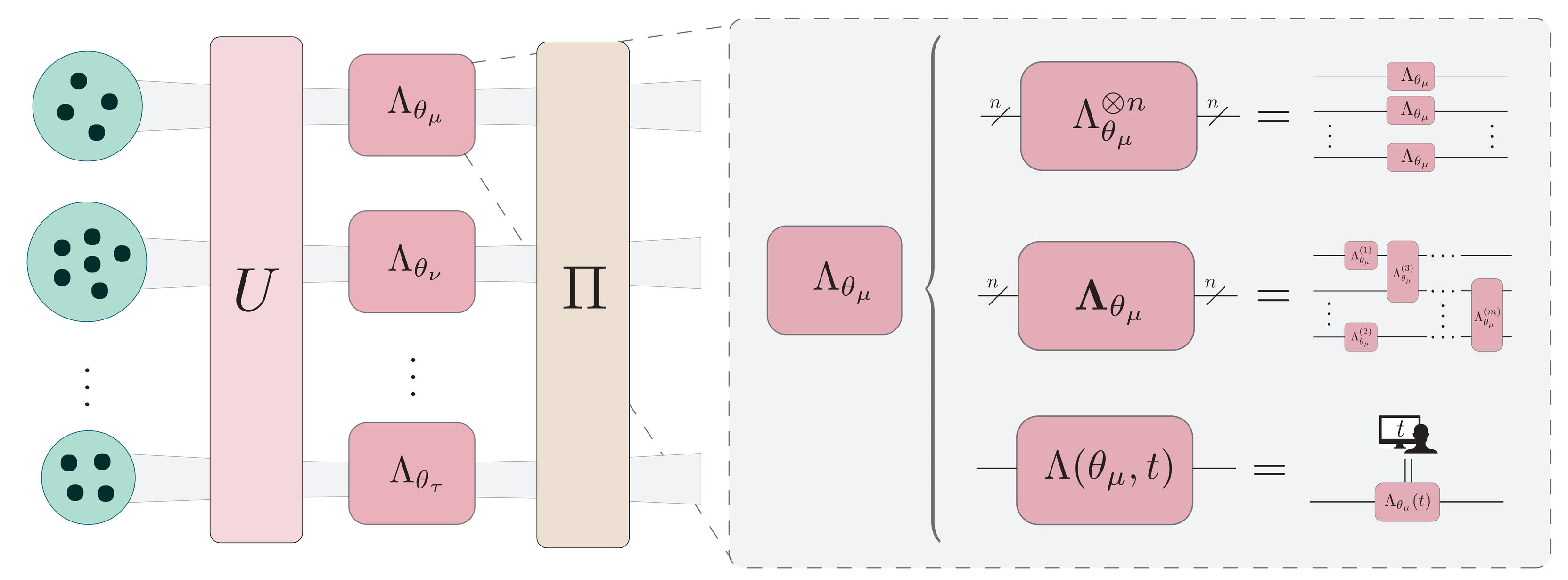
DEFINITION: (*Privacy*) The privacy measure of a multi-parameter estimation problem, is a function of the quantum Fisher information matrix (QFI) and the vector providing the target function. It is given by:

$$\mathcal{P}(\mathcal{Q}, a) = \frac{a^T \mathcal{Q} a}{\|\vec{a}\|^2 \operatorname{Tr} \mathcal{Q}}$$

The question of finding these private states then becomes intertwined with the dynamics governing the evolution, seen from the QFI matrix.

How to Build Private and Robust States?

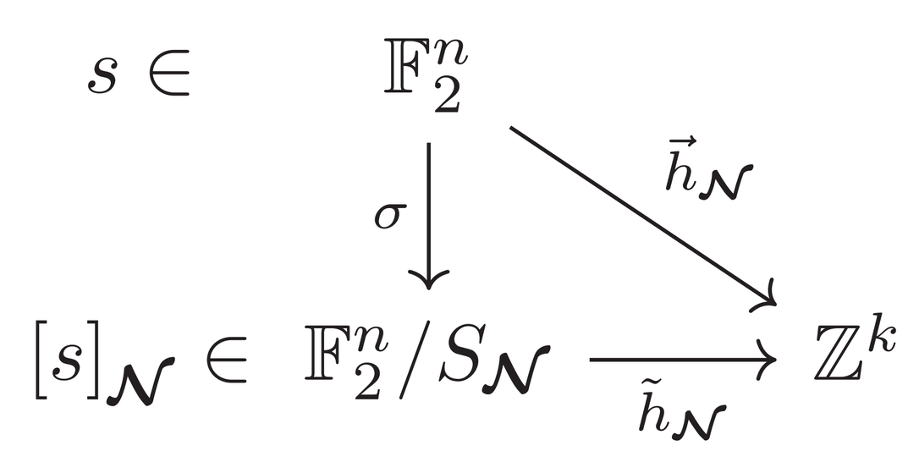
ASSUMPTIONS:



TOOLS:

$\vec{h}_{\mathcal{N}}(s)$ - Distributed Hamming-weight

$s \in \{0,1\}^{\times n}, \mathcal{N}$ a partition of $[n]$

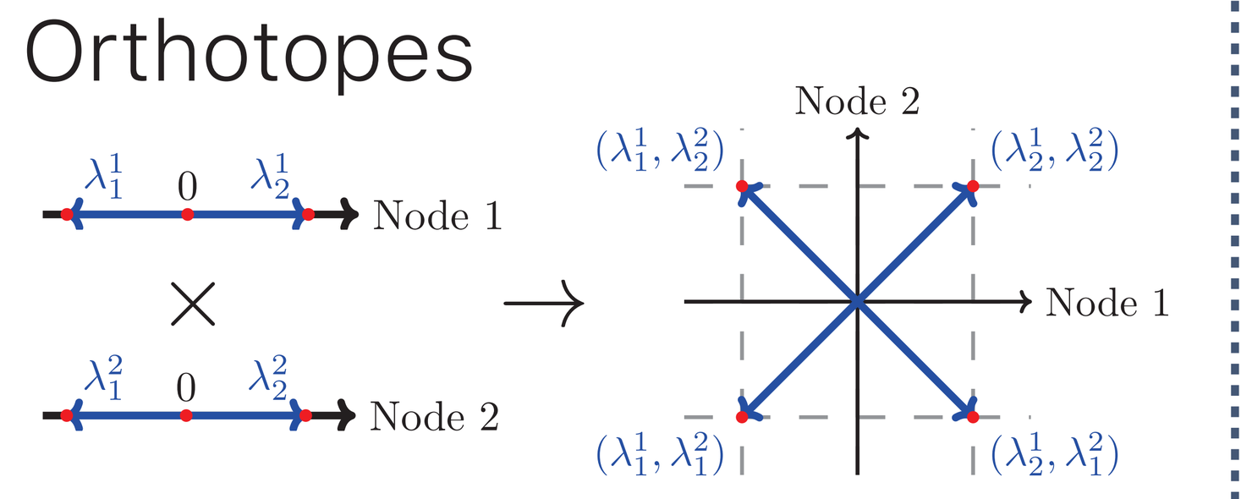


Invariance under local permutations!

Local Hamiltonians

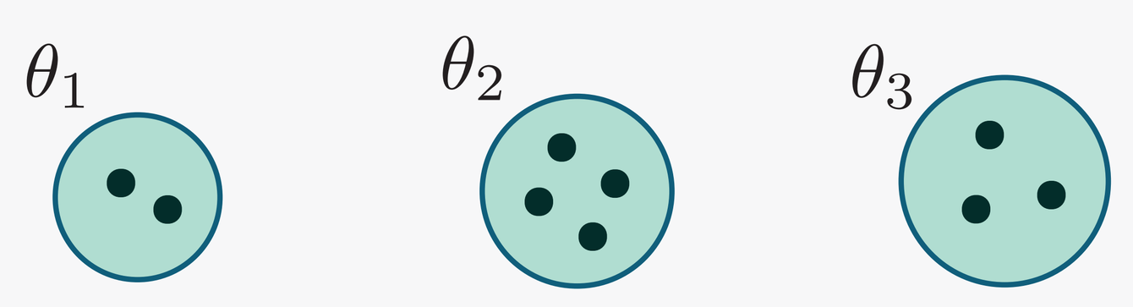
$$\boldsymbol{H}_\mu |\lambda_j^\mu\rangle = \lambda_j^\mu |\lambda_j^\mu\rangle \rightarrow \begin{cases} \mathcal{B}^\mu = \{|\lambda_j^\mu\rangle\}_{j\in\mu}, \\ \mathcal{O}^\mu = \{\lambda_j^\mu\}_{j\in\mu}. \end{cases}$$

Orthotopes



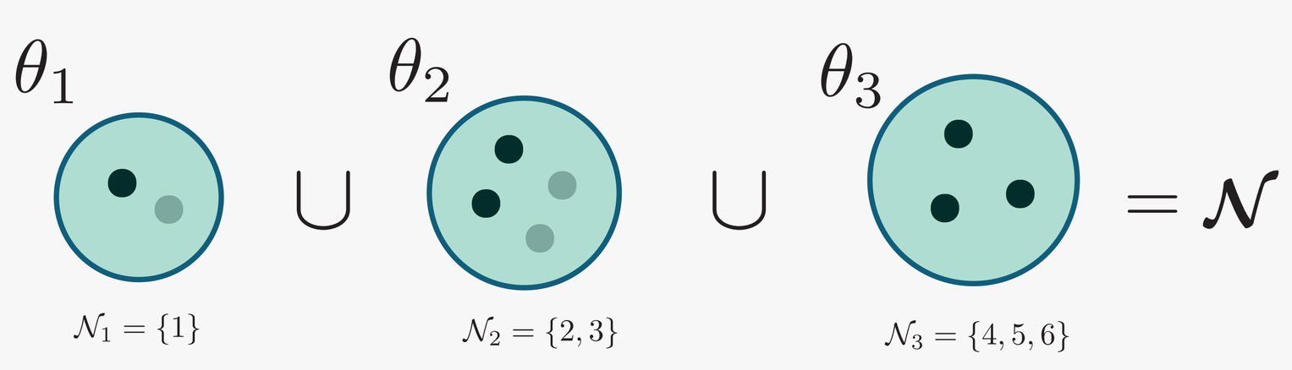
Separable Hamiltonians

Step 1: *Verify if we have sufficient qubits for the target function*



$$gcd(\vec{a}) = gcd(a_1, a_2, \cdots, a_k) = 1$$
$$\vec{n} = (2,4,3) \succeq \vec{a} = (1,2,3)$$

Step 2: *Build first private state family with minimal resources*



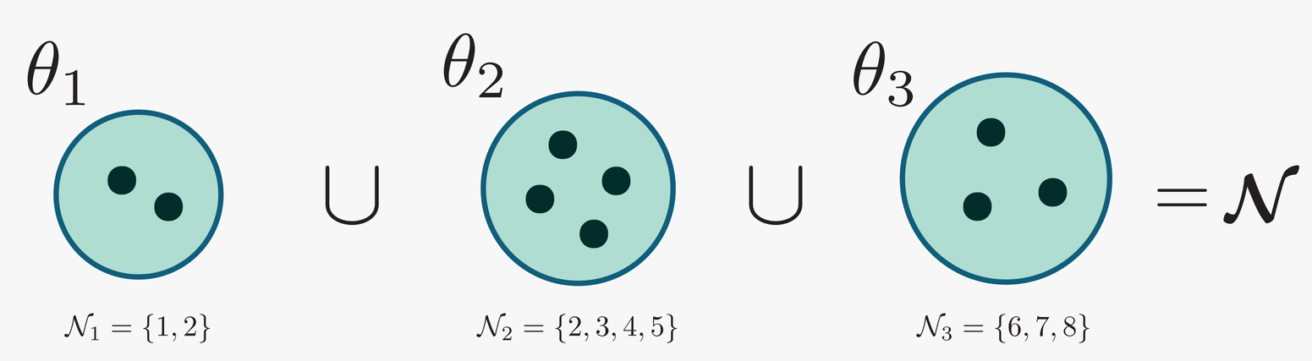
$n = 1+2+3, s \in \{0,1\}^n$

$s_0 = (0\ 00\ 000) \quad s_1 = (1\ 11\ 111)$

Such that: $\vec{h}_{\mathcal{N}}(s_1) - \vec{h}_{\mathcal{N}}(s_0) = \vec{a}$

$$\mathcal{F} = \{\alpha |s_0\rangle + \beta |s_1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

Step 3: *Build robust and private families by adding extra qubits*



$n = 2+4+3, s \in \{0,1\}^n$

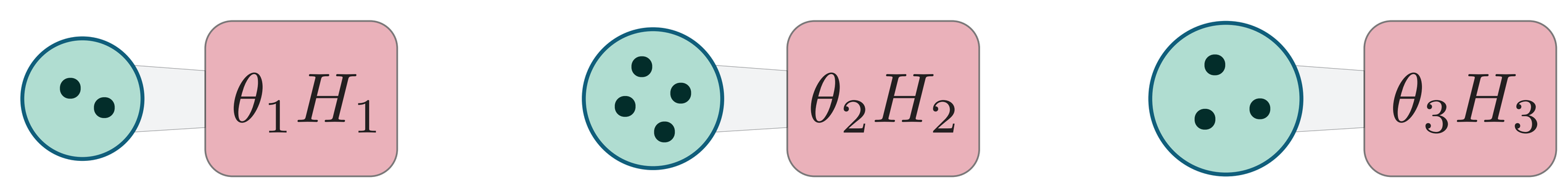
$s_0^0 = (00\ 0000\ 000), s_1^0 = (10\ 1100\ 111)$
$s_0^1 = (00\ 0001\ 000), s_1^1 = (10\ 1101\ 111)$
$s_0^2 = (00\ 0011\ 000), s_1^2 = (10\ 1111\ 111)$
$s_0^3 = (01\ 0000\ 000), s_1^3 = (11\ 1100\ 111)$
$s_0^4 = (01\ 0001\ 000), s_1^4 = (11\ 1101\ 111)$
$s_0^5 = (01\ 0011\ 000), s_1^5 = (11\ 1111\ 111)$

Such that: $\vec{h}_{\mathcal{N}}(s_1^j) - \vec{h}_{\mathcal{N}}(s_0^j) = \vec{a}, \ \forall j$

$$\mathcal{F}_j = \left\{ \sum_{\sigma\in S_{\mathcal{N}}} \alpha_\sigma \left|\sigma(s_0^j)\right\rangle + \sum_{\sigma\in S_{\mathcal{N}}} \beta_\sigma \left|\sigma(s_1^j)\right\rangle, \alpha_\sigma, \beta_\sigma \in \mathbb{C}, \text{normalized} \right\}$$

General Local Hamiltonians

Step 1: *Identify the local eigenstates and eigenvalues*

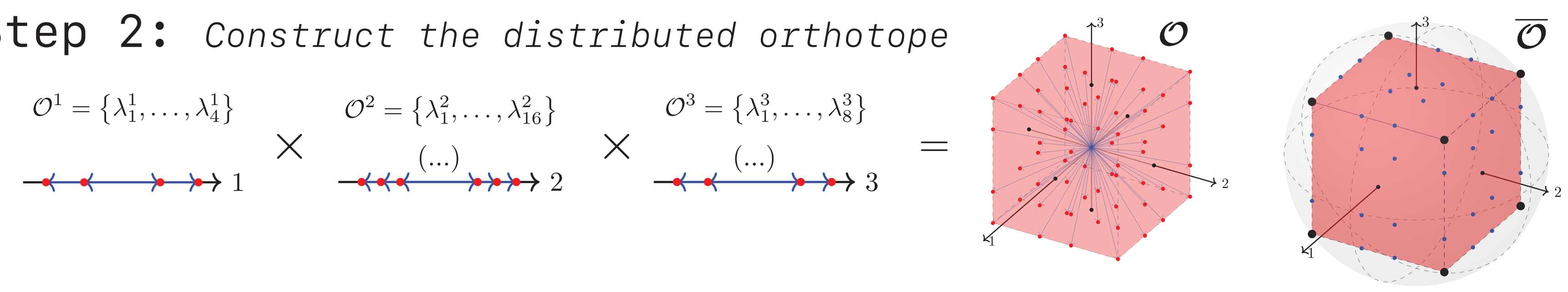


$\mathcal{B}^1 = \{|\lambda_1^1\rangle, \ldots, |\lambda_4^1\rangle\}$, $\mathcal{O}^1 = \{\lambda_1^1, \ldots, \lambda_4^1\}$

$\mathcal{B}^2 = \{|\lambda_1^2\rangle, \ldots, |\lambda_{16}^2\rangle\}$, $\mathcal{O}^2 = \{\lambda_1^2, \ldots, \lambda_{16}^2\}$

$\mathcal{B}^3 = \{|\lambda_1^3\rangle, \ldots, |\lambda_8^3\rangle\}$, $\mathcal{O}^3 = \{\lambda_1^3, \ldots, \lambda_8^3\}$

Step 2: *Construct the distributed orthotope*



Step 3: *Construct the private orthotope and states*

$$\mathcal{O}_-^2 = \{\vec{v} - \vec{w} : \forall \vec{v}, \vec{w} \in \mathcal{O}\}$$

Results:

- A **method** to build private states under hamiltonian dynamics;
- **Proofs** that these are in fact the **only** private states that exist;
- Link between the Hamiltonian and the private states structure - **the private orthotope.**

Target	Hamiltonian	Resources	Private Family	Theorem
$\vec{a} \in \mathbb{R}^k$	Controlable (Fig. 2 d))	$\vec{n} = \vec{1}$	GHZ State	Thm. 3.4
$\vec{a} \in \mathbb{N}^k$	Separable (Fig. 2 a))	Zone (I)	None	Thms. 3.1, 3.3
		Zone (II)	GHZ State	Thms. 3.2, 3.4
		Zone (III)	Ancilla-Private States	Thm. 3.5
		Zone (IV)	Private Logical States	Thm. 3.6
$\vec{a} \in \mathcal{O}_-^2$	General (Fig. 2 b))	Depends on H	$\exists$ Private State	Thm. 3.7

Fundação para a Ciência e a Tecnologia

Acknowledgments:
The authors acknowledge the support from the EU Quantum Flagship project QIA (101102140) and France 2030 under the French National Research Agency projects HQI ANR-22-PNCQ-0002 and the PEPR integrated project EPiQ ANR-22-PETQ-0007. L.B. and Y.O. thank the support from Fundação para a Ciência e a Tecnologia (FCT, Portugal), namely through project UIDB/04540/2020. L.B. acknowledges the support of FCT through scholarship BD/05268/2021.