



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

Padua Research Archive - Institutional Repository

Consensus for Quantum Networks: Symmetry from Gossip Interactions

Original Citation:

Availability:

This version is available at: 11577/3042665 since:

Publisher:

Published version:

DOI: 10.1109/TAC.2014.2336351

Terms of use:

Open Access

This article is made available under terms and conditions applicable to Open Access Guidelines, as described at <http://www.unipd.it/download/file/fid/55401> (Italian only)

(Article begins on next page)

Consensus for Quantum Networks: From Symmetry to Gossip Iterations

Luca Mazzarella, Alain Sarlette, Francesco Ticozzi

Abstract—This paper extends the consensus framework, widely studied in the literature on distributed computing and control algorithms, to networks of quantum systems. We define consensus situations on the basis of invariance and symmetry properties, finding four different probabilistic generalizations of classical consensus states. We then extend the gossip consensus algorithm to the quantum setting and prove its convergence properties, showing how it converges to symmetric states while preserving the expectation of permutation-invariant global observables.

Index Terms—Consensus, Quantum Information and Control, Markov Processes, Distributed Algorithms.

I. INTRODUCTION

Among the recent trends in control and systems theory, the field of distributed control, estimation and optimization on networks has stimulated an impressive amount of research, see e.g. [1], [2], [3], [4], [5], [6], [7], [8], [9]. A basic task for distributed information processing is reaching *consensus* on some common control objective, shared value or slack variable. The present paper extends this well-studied consensus problem (see e.g. [10], [11], [12], [13]) to networks of quantum systems, a special case of which would be classical probability distributions.

Exploring the links between information processing tasks and stochastic dynamics on networks has recently opened new research directions towards “distributed” quantum information applications. Among these, we recall quantum computation [14], [15] in its potential implementation via dissipative means [16], and its connection to quantum random walks [17], [18]. Other specific tasks include noise protection and dynamical error-correction [19], [20], [21], [22], [23], entanglement generation through stabilizing dissipative dynamics [24], [25], the creation of quantum “gadgets” driven by dissipation [26], as well as most tasks in the control of open quantum systems [27], [28], [29], [30], [31].

In this spirit, we here develop a framework for addressing quantum consensus problems: we identify and characterize a hierarchy of quantum consensus situations and study how these can be reached by suitable dissipative quantum dynamics, while preserving some global information on the network. Our work offers not only a formal generalization of the well-known

classical consensus problem, along with some intriguing insights on the latter, but also a potentially new viewpoint on a number of issues in quantum information. More specifically, it ties the structure of symmetric states and correlations [32], [33] to their potential generation via quasi-local resources [25], and to the relaxation of many-body systems to thermal states. While this work is mainly meant to provide solid theoretical foundation to quantum consensus problems, links between the proposed theory and potential applications will be outlined in the conclusions. As an interesting by-product, the present work also provides a viewpoint on consensus for classical systems in the context of probability distributions instead of deterministic states.

An attempt to lift the consensus problem to the quantum domain has been presented in [34]. It is based on a “cone geometry” approach, viewing quantum Kraus maps as the non-commutative generalization of Markov chains that model consensus algorithms. The authors show how Birkhoff’s Theorem and Hilbert’s projective metric lead to a general convergence result and contraction ratio estimation. However, by describing the dynamics of the whole system of interest as governed by a single Markov transition mechanism, this formulation does not account for subsystem structure or network connections in the quantum setting. It therefore defines consensus as asymptotic convergence to a scalar multiple of the identity: for quantum states this corresponds to a fully mixed, most uncertain state which is not the typical desired target for quantum information processing applications.

In the present paper, we approach quantum consensus from an “operational”, multi-agent control perspective, starting from the basic classical ingredients: a network of subsystems, an interaction protocol with locality constraints, and a target consensus situation. As a first step, Section II provides four possible ways to generalize the concept of a *consensus state* to the quantum domain and explores their connections, establishing a hierarchy of quantum consensus definitions. Section III presents the quantum open-system dynamics and the locality notions that we employ to describe the interactions between the quantum “agents”. Typical methods for interaction selection and timing are also introduced, in analogy with classical consensus. This provides all the ingredients needed to specify the general properties of an evolution that achieves *quantum average consensus*. The symmetry-based reformulations at each step provide an alternative interpretation of classical consensus, and in Section IV this leads us to a quantum generalization of the classical gossip algorithm. We prove its *convergence to symmetric-state consensus* while preserving the expectation of any permutation-invariant observable. We further show how the algorithm can be explicitly seen as a

L. Mazzarella is with Dipartimento di Ingegneria dell’Informazione, Università di Padova, via Gradenigo 6/B, 35131 Padova, Italy (mazzarella@dei.unipd.it).

A. Sarlette is with SYSTeMS, Ghent University, Technologiepark Zwijsnaarde 914, 9052 Gent, Belgium (alain.sarlette@ugent.be).

F. Ticozzi is with Dipartimento di Ingegneria dell’Informazione, Università di Padova, via Gradenigo 6/B, 35131 Padova, Italy (ticozzi@dei.unipd.it) and Dept. of Physics and Astronomy, Dartmouth College, 6127 Wilder, 03755 Hanover, NH (USA).

Work partially supported by the University of Padua QFUTURE grant.

generalization of the classical one and the classical convergence results can be used to prove a weaker convergence property. The section concludes with an example of the gossip algorithm working on a four-qubit network. In Section V we summarize the main results and provide an outlook on possible developments and applications for our framework. A small tutorial on quantum systems modeling is given in Appendix A, along with an overview of the notations and conventions we use.

II. CONSENSUS STATES

A classical *consensus state* for a multipartite system is one in which the states of all the subsystems, often called agents, are the same (although not necessarily stationary). Since in general a quantum state for a multipartite system cannot be factorized into subsystem states (see Appendix A), the definition of consensus must be carefully reconsidered. We here present an operational approach that leads to a hierarchy of definitions for what can be claimed to be “quantum consensus”.

A. Defining Classical Consensus

The consensus problem for classical systems is most typically formulated along the following lines [10], [12]. Consider m subsystems, each one associated to a state given by a configuration variable $x_k \in \mathbb{R}^n$. These subsystems evolve through bilateral interactions, according to some networking scheme and dynamics (see Section IV), and reach a *consensus state* if they converge to the set $\mathcal{C} = \{(x_1, x_2, \dots, x_m) : x_j = x_k \forall j, k\}$. Furthermore, the agents are said to compute an *average consensus* if for given initial states $(x_1(0), x_2(0), \dots, x_m(0))$ they converge to the particular equilibrium $(\bar{x}, \bar{x}, \dots, \bar{x}) \in \mathcal{C}$ where $\bar{x} = \frac{1}{m} \sum_i x_i(0)$.

Alternatively, consensus can be characterized as invariance w.r.t. subsystem permutations. Let \mathfrak{P} denote the set of all subsystem permutation operators, i.e. each $P_\pi \in \mathfrak{P}$ is associated to some permutation π of the integers $1, 2, \dots, m$ such that $P_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$ for any x_1, x_2, \dots, x_m . Denoting the joint state of the $x_k \in \mathbb{R}^n$ by a vector $x \in \mathbb{R}^{mn}$, each $P_\pi \in \mathfrak{P}$ can be written as an $mn \times mn$ matrix resulting from the Kronecker product of some $m \times m$ permutation matrix with the $n \times n$ identity matrix. Then we can define consensus as:

$$\mathcal{C} = \{x \in \mathbb{R}^{mn} : P_\pi x = x \text{ for all } P_\pi \in \mathfrak{P}\}. \quad (1)$$

It is standard that checking $P_\pi x = x$ for all pairwise permutations P_π is sufficient to guarantee $P_\pi x = x$ for all $P_\pi \in \mathfrak{P}$.

Average consensus is a fundamental element of distributed computation because for each linear function $Q : \mathbb{R}^{mn} \rightarrow \mathbb{R}^s$ which is invariant under all subsystem permutations, there exists $q : \mathbb{R}^n \rightarrow \mathbb{R}^s$ such that $Qx = q\bar{x}$. Thus such Q can be evaluated locally by each agent once they have reached average consensus. The fact that all permutations can be obtained by concatenating pairwise permutations, already suggests that average consensus is computable with standard distributed algorithms.

B. Quantum Consensus Definitions and their Relationships

Defining what a consensus situation ought to be in a quantum “network” is not a straightforward task. More than one definition may be appropriate depending on the type of *symmetry* we are seeking. Following the analogy with the classical case can help, but quantum measurement outcomes are intrinsically stochastic, so we must consider *probabilistic* consensus situations from the beginning. Let us explore different options by first discussing a simple case.

Example 1: When is a quantum network in consensus?

Consider a multipartite quantum system composed of three qubits, with associated Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, and three observables of the form $\sigma^{(1)} = \sigma_z \otimes I \otimes I$, $\sigma^{(2)} = I \otimes \sigma_z \otimes I$, $\sigma^{(3)} = I \otimes I \otimes \sigma_z$, where the Pauli matrix $\sigma_z = \text{diag}(1, -1)$.¹ These correspond to observables of the quantity associated to σ_z for each of the subsystems. It seems natural to say that the system is in consensus with respect to the expectation of σ_z if

$$\text{Tr}(\rho\sigma^{(1)}) = \text{Tr}(\rho\sigma^{(2)}) = \text{Tr}(\rho\sigma^{(3)}). \quad (2)$$

The conditions for this to happen can be worked out explicitly in terms of the diagonal elements of the state ρ . In particular it is easy to check that all the following states satisfy condition (2):

$$\begin{aligned} \rho^A &= \frac{1}{8} I \otimes (|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \otimes (|0\rangle + |1\rangle)(\langle 0| + \langle 1|); \\ \rho^B &= \frac{1}{4} I \otimes (|0, 0\rangle + |1, 1\rangle)(\langle 0, 0| + \langle 1, 1|); \\ \rho^C &= \frac{1}{8} I \otimes I \otimes I; \\ \rho^D &= \frac{1}{2} (|0, 0, 0\rangle\langle 0, 0, 0| + |1, 1, 1\rangle\langle 1, 1, 1|); \\ \rho^E &= |0, 0, 0\rangle\langle 0, 0, 0|; \\ \rho^F &= \frac{1}{2} (|0, 0, 0\rangle + |1, 1, 1\rangle)(\langle 0, 0, 0| + \langle 1, 1, 1|). \end{aligned}$$

All these states, except ρ^E , have $\text{Tr}(\rho\sigma^{(i)}) = 0$ for $i = 1, 2, 3$.

The above requirement can be strengthened by requesting (2) to hold when σ_z is replaced by *any* observable $\sigma \in \mathfrak{B}(\mathbb{C}^2)$ in the definition of $\sigma^{(1)}, \sigma^{(2)}, \sigma^{(3)}$. This is equivalent to imposing that the reduced states for the three subsystems are the same (a formal proof is provided in the next subsection). It is then easy to check that $\rho^B, \rho^C, \rho^D, \rho^E, \rho^F$ satisfy this requirement, while ρ^A does not. In fact the reduced states for ρ^A are:

$$\rho_1^A = \frac{1}{2} I, \quad \rho_2^A = \rho_3^A = \frac{1}{2} (|0\rangle + |1\rangle)(\langle 0| + \langle 1|).$$

In the light of (1), another potential definition of quantum consensus would require the *state to be symmetric*, i.e. invariant under any permutations of the subsystems. This choice can be motivated by the classical case, where the consensus state

¹A qubit is a quantum system associated to a two-dimensional Hilbert space $\mathcal{H} \sim \mathbb{C}^2$; a standard basis for the latter is conventionally given by the vectors $\{|0\rangle, |1\rangle\} \subset \mathcal{H}$. The traceless unitary and hermitian Pauli operators $\sigma_x, \sigma_y, \sigma_z$, completed with the identity operator, form an orthonormal basis for the operators on \mathcal{H} . Explicitly, $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$, $\sigma_y = i|1\rangle\langle 0| - i|0\rangle\langle 1|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

is indeed permutation invariant. Among the states defined in Example 1, only $\rho^C, \rho^D, \rho^E, \rho^F$ are permutation invariant.

Lastly, one might desire to have subsystem agreement not only on the observable averages, but also *on each measurement*. Namely, we want that each projective measurement of the (commuting and hence compatible) observables $\sigma_1, \sigma_2, \sigma_3$ gives *perfectly correlated results* for the three subsystems. That is, among all possible measurement results $\{-1, +1\}^{\times 3}$, only $(-1, -1, -1)$ and $(+1, +1, +1)$ have a nonzero probability to occur². For instance if the system is in an entangled state of the form $\rho = (\alpha|0, 0, 0\rangle + \beta|1, 1, 1\rangle)(\alpha^*\langle 0, 0, 0| + \beta^*\langle 1, 1, 1|)$, with $|\alpha|^2 + |\beta|^2 = 1$, the outcome of a measurement operation is $(-1, -1, -1)$ with probability $|\alpha|^2$ and $(+1, +1, +1)$ with probability $|\beta|^2$. With $\alpha = \beta = \frac{1}{\sqrt{2}}$ we get ρ^F above. The states ρ^A, ρ^B and ρ^C do not satisfy this definition of consensus; indeed, for these three states, the distribution of measurement results for qubit 1 is independent of the measurements on the other two qubits, e.g. $(+1, -1, -1)$ and $(-1, -1, -1)$ have the same nonzero probability so uncorrelated measurement results can happen. Note however that also mixed states can lead to correlated results, if they express perfect classical correlations, as is the case for any state of the form $\rho^G = p|0, 0 \dots 0\rangle\langle 0, 0 \dots 0| + (1-p)|1, 1 \dots 1\rangle\langle 1, 1 \dots 1|$ with $0 < p < 1$. For three qubits with $p = \frac{1}{2}$ we get ρ^D above. \square

Let us formalize the ideas emerging from the former example. Consider a multipartite system composed of m isomorphic subsystems, labeled with indices $i = 1, \dots, m$, with associated Hilbert space $\mathcal{H}^m := \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_m \simeq \mathcal{H}^{\otimes m}$, with $\dim(\mathcal{H}_i) = \dim(\mathcal{H}) = n$ and $n \geq 2$. We shall refer to this multipartite system as to our *quantum network*. For any operator $X \in \mathfrak{B}(\mathcal{H})$, we will denote by $X^{\otimes m}$ the tensor product $X \otimes X \otimes \dots \otimes X$ with m factors. Given an operator $\sigma \in \mathfrak{B}(\mathcal{H})$, we denote by $\sigma^{(i)}$ the local operator:

$$\sigma^{(i)} := I^{\otimes(i-1)} \otimes \sigma \otimes I^{\otimes(m-i)}.$$

Permutations of quantum subsystems are expressed by a unitary operator $U_\pi \in \mathcal{U}(\mathcal{H})$, which is uniquely defined by

$$U_\pi(X_1 \otimes \dots \otimes X_m)U_\pi^\dagger = X_{\pi(1)} \otimes \dots \otimes X_{\pi(m)}$$

for any operators X_1, \dots, X_m in $\mathfrak{B}(\mathcal{H})$, where π is a permutation of the first m integers. A state or observable is said to be *permutation invariant* if it commutes with all the subsystem permutations. It is worth noting that given any observable $Q \in \mathfrak{H}(\mathcal{H}^m)$, we can define a permutation invariant observable X by considering:

$$X = \frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi^\dagger Q U_\pi. \quad (3)$$

²The set $\{c_1, c_2, c_3, \dots\}^{\times n}$ is the cartesian product of $\{c_1, c_2, c_3, \dots\}$ by itself n times, i.e. the set of n -tuples with components taken from $\{c_1, c_2, c_3, \dots\}$.

Definition 1 (σ EC): Given $\sigma \in \mathfrak{B}(\mathcal{H})$, a state $\rho \in \mathfrak{D}(\mathcal{H}^m)$ is in σ -Expectation Consensus (σ EC) if:

$$\text{Tr}(\sigma^{(1)}\rho) = \dots = \text{Tr}(\sigma^{(k)}\rho).$$

Definition 2 (RSC): A state $\rho \in \mathfrak{D}(\mathcal{H}^m)$ is in *Reduced State Consensus* (RSC) if, defining the reduced states $\bar{\rho}_k = \text{Tr}(\otimes_{j \neq k} \mathcal{H}_j)(\rho)$, we have

$$\bar{\rho}_1 = \dots = \bar{\rho}_m.$$

Definition 3 (SSC): A state $\rho \in \mathfrak{D}(\mathcal{H}^m)$ is in *Symmetric State Consensus* (SSC) if for each unitary permutation U_π we have

$$U_\pi \rho U_\pi^\dagger = \rho$$

Definition 4 (σ SMC): Given an observable σ with spectral decomposition $\sigma = \sum_j s_j \Pi_j \in \mathfrak{D}(\mathcal{H})$, all s_j different, a state $\rho \in \mathfrak{D}(\mathcal{H}^m)$ is in *Single σ -Measurement Consensus* (σ SMC) if:

$$\text{Tr}(\Pi_j^{(k)} \Pi_j^{(\ell)} \rho) = \text{Tr}(\Pi_j^{(\ell)} \rho), \quad (4)$$

for all $k, \ell \in \{1, \dots, m\}$, and for each j .

The definition of σ SMC requires that the outcomes of σ measurements on different subsystems be exactly the same *for each trial*. Indeed, in this last definition, the right-hand side of (4) is the probability of obtaining s_j as a measurement result on both subsystem ℓ and k (note that $\Pi_j^{(k)}$ and $\Pi_j^{(\ell)}$ commute, so this joint measurement $\Pi_j^{(k)} \Pi_j^{(\ell)}$ is well-defined). If those two probabilities are equal, then necessarily the probability of s_j on k conditional to observing s_j on ℓ is one (assuming that $\Pi_j^{(\ell)} \rho \Pi_j^{(\ell)} \neq 0$; that special case is trivial and can be treated separately).

One may wonder why, as we did for the consensus in expectation, we did not try to strengthen the σ SMC property, requiring perfect correlations of outcomes for *any* local measurements. In fact it can be shown that states satisfying this property do not exist.

Proposition 1: For any finite-dimensional quantum system, there does not exist a state ρ that satisfies σ SMC for all σ . The proof makes use of Proposition 4 below, thus we postpone it to Appendix C. \square

Remark: It is worth remarking how all these definitions could be given for classical systems, in the context of consensus for random variables or for probability distributions of the state values. In this case, for example, σ EC would require the expectation of a set of random variables, each one associated to a subsystem, to be the same in all subsystems; RSC would require the marginal distributions on each subsystem to be equal; and SSC would require that the joint probability distribution is invariant with respect to subsystem permutations. In some sense the definition of σ SMC is the closest to the classical case, as it requires perfect agreement on the outcome of a set of random variables for *each measurement*.

All the states in our example satisfy σ_z EC, all but ρ^A satisfy RSC, ρ^C to ρ^F satisfy SSC, and ρ^D to ρ^F satisfy σ_z SMC. There obviously seems to be a hierarchy in these definitions, and the following properties are meant to better characterize them. We shall use the notation $\mathcal{C}_{XYZ} \subset \mathfrak{D}(\mathcal{H})$ to indicate the set of states that satisfy the properties of the acronym XYZ,

e.g. \mathcal{C}_{RSC} is the set of all Reduced State Consensus states. Note that, since all consensus definitions involve linear constraints, the consensus sets are all convex.

Theorem 1: The following chain of implications holds:

$$\text{SSC} \implies \text{RSC} \implies \sigma\text{EC},$$

while the converse implications are not true in general.

Proof: $\text{SSC} \implies \text{RSC}$: If $U_\pi \rho U_\pi^\dagger = \rho$ for each permutation, consider in particular $U_{(\ell,k)}$ that swaps subsystems ℓ and k . Then

$$\bar{\rho}_k = \text{Tr}_{\otimes_{j \neq k} \mathcal{H}_j}(\rho) = \text{Tr}_{\otimes_{j \neq k} \mathcal{H}_j}(U_{(\ell,k)} \rho U_{(\ell,k)}^\dagger) = \bar{\rho}_\ell,$$

and the reasoning can be repeated for any pair. $\text{RSC} \implies \text{OSC}$ is immediate by definition. States ρ^B and ρ^A from Example 1 provide counterexamples for the converse of the first and of the second implication, respectively. \square

The converse result for the relation between RSC and σEC goes as follows.

Proposition 2: A state is RSC if and only if it is σEC for all $\sigma \in \mathfrak{B}(\mathcal{H})$.

Proof: RSC implies σEC for all σ by definition. Conversely, assume ρ to be σEC for any σ . The reduced state for any subsystem can be written as $\bar{\rho}_k = \sum_\ell \text{Tr}(\rho \sigma_\ell^{(k)}) \sigma_\ell$, where $\{\sigma_\ell\}$ is an orthogonal, hermitian basis of operators for $\mathfrak{B}(\mathcal{H})$. Since by hypothesis $\text{Tr}(\rho \sigma_\ell^{(k)})$ does not depend on k , then all the reduced states are identical. \square

A converse result for the relation between RSC and SSC cannot be set up in general. Instead, we have the following property.

Proposition 3: RSC states with $\bar{\rho}_k$ a pure state for each k are also SSC states.

Proof: If $\bar{\rho}_k$ is a pure state for each k , then necessarily $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_m\rangle$ for some $|\psi_k\rangle$, $k = 1, 2, \dots, m$. If in addition we require RSC, then we need $|\psi_k\rangle\langle\psi_k| = \bar{\rho}_k = \bar{\rho}_j = |\psi_j\rangle\langle\psi_j|$ for all j, k , thus $|\psi_k\rangle = |\psi_j\rangle$ up to an irrelevant phase factor for all j, k and particle permutation indeed leaves $|\psi\rangle$ invariant. \square

The structure of the σSMC states is further characterized in the following proposition.

Proposition 4: A state is in σSMC if and only if, defining $\Pi_{\text{sym}} = \sum_j \Pi_j^{\otimes m}$, it holds

$$\text{Tr}(\Pi_{\text{sym}} \rho) = 1, \quad (5)$$

or equivalently

$$\Pi_{\text{sym}} \rho \Pi_{\text{sym}} = \Pi_{\text{sym}} \rho = \rho. \quad (6)$$

Proof: Note that the properties $\text{Tr}(\Pi_{\text{sym}} \rho) = 1$ and $\Pi_{\text{sym}} \rho \Pi_{\text{sym}} = \Pi_{\text{sym}} \rho = \rho$ are equivalent because Π_{sym} is an orthonormal projector and ρ is self-adjoint positive semi-definite with unit trace. Assume (5) to hold. Along with the

identities $\Pi_j^{(k)} \Pi_{\text{sym}} = \Pi_j^{(k)} \Pi_j^{\otimes m} = \Pi_j^{\otimes m}$, this gives:

$$\begin{aligned} \text{Tr}(\Pi_j^{(\ell)} \Pi_j^{(k)} \rho) &= \text{Tr}(\Pi_j^{(\ell)} \Pi_j^{(k)} \Pi_{\text{sym}} \rho) \\ &= \text{Tr}(\Pi_j^{(\ell)} \Pi_j^{\otimes m} \rho) \\ &= \text{Tr}(\Pi_j^{(\ell)} \Pi_{\text{sym}} \rho) \\ &= \text{Tr}(\Pi_j^{(\ell)} \rho), \end{aligned}$$

for all j, k, ℓ . Hence, the SMC definition (4) indeed holds. On the other hand, suppose that (5) does not hold. This means that $\text{Tr}((I - \Pi_{\text{sym}}) \rho) > 0$. We want to show that this implies

$$\text{Tr}(\Pi_j^{(k)} \Pi_j^{(\ell)} \rho) \neq \text{Tr}(\Pi_j^{(\ell)} \rho)$$

for some j, k, ℓ . Let us write

$$I - \Pi_{\text{sym}} = \sum_{j_1, \dots, j_m \text{ except } \{j_1 = \dots = j_m\}} \Pi_{j_1} \otimes \dots \otimes \Pi_{j_m}.$$

Since $\text{Tr}((I - \Pi_{\text{sym}}) \rho) > 0$ implies that $\text{Tr}(\Pi_{j_1} \otimes \dots \otimes \Pi_{j_m} \rho) > 0$ for at least one of the terms in the above sum, let us take one such term, denote the corresponding indices as $\{\bar{j}_s\}$ and denote by k, ℓ two subsystems such that $\bar{j}_k \neq \bar{j}_\ell$ in that term. Now writing $\Pi_{\bar{j}_1} \otimes \dots \otimes \Pi_{\bar{j}_m} = \Pi_{\bar{j}_1}^{(1)} \Pi_{\bar{j}_2}^{(2)} \dots \Pi_{\bar{j}_m}^{(m)}$, where all factors commute, we have:

$$\text{Tr}(\Pi_{\bar{j}_k}^{(k)} \Pi_{\bar{j}_\ell}^{(\ell)} \rho) \geq \text{Tr}(\Pi_{\bar{j}_1}^{(1)} \Pi_{\bar{j}_2}^{(2)} \dots \Pi_{\bar{j}_m}^{(m)} \rho) > 0.$$

Exploiting basic projection properties we thus get:

$$\begin{aligned} \text{Tr}(\Pi_{\bar{j}_\ell}^{(k)} \Pi_{\bar{j}_\ell}^{(\ell)} \rho) &\leq \text{Tr}((1 - \Pi_{\bar{j}_k}^{(k)}) \Pi_{\bar{j}_\ell}^{(\ell)} \rho) \\ &= \text{Tr}(\Pi_{\bar{j}_\ell}^{(\ell)} \rho) - \text{Tr}(\Pi_{\bar{j}_k}^{(k)} \Pi_{\bar{j}_\ell}^{(\ell)} \rho) \\ &\leq \text{Tr}(\Pi_{\bar{j}_\ell}^{(\ell)} \rho) - \text{Tr}(\Pi_{\bar{j}_1}^{(1)} \Pi_{\bar{j}_2}^{(2)} \dots \Pi_{\bar{j}_m}^{(m)} \rho) \\ &< \text{Tr}(\Pi_{\bar{j}_\ell}^{(\ell)} \rho). \end{aligned}$$

\square

To conclude, the following proposition connects σSMC to the other properties.

Proposition 5: (a) σSMC implies σEC , while the converse is not true.

(b) σSMC for a σ with nondegenerate spectrum implies RSC, while the converse is not true.

(c) σSMC for a σ with nondegenerate spectrum implies SSC, while the converse is not true.

Proof: For (a), we have since (4) holds for all k, ℓ :

$$\text{Tr}(\Pi_j^{(k)} \rho) = \text{Tr}(\Pi_j^{(k)} \Pi_j^{(\ell)} \rho) = \text{Tr}(\Pi_j^{(\ell)} \rho).$$

By linearity, we thus have:

$$\begin{aligned} \text{Tr}(\sigma^{(k)} \rho) &= \sum_j s_j \text{Tr}(\Pi_j^{(k)} \rho) = \sum_j s_j \text{Tr}(\Pi_j^{(\ell)} \rho) \\ &= \text{Tr}(\sigma^{(\ell)} \rho). \end{aligned}$$

A counterexample for the converse is state ρ^A in Example 1.

Counterexamples for the converse of (b) and (c) are respectively states ρ^B and ρ^C in Example 1. For the direct statements, given Proposition 1, we know that if (c) is true, then (b) must be true as well. Let us then focus on (c). Take the

representation of ρ in the basis associated to $\sigma = \sum_j s_j |j\rangle\langle j|$, where thus $|j\rangle\langle j| = \Pi_j$, that reads

$$\rho = \sum_{\substack{j_1, j_2, \dots, j_m, \\ k_1, k_2, \dots, k_m}} r_{\substack{j_1, j_2, \dots, j_m, \\ k_1, k_2, \dots, k_m}} |j_1, j_2, \dots, j_m\rangle\langle k_1, k_2, \dots, k_m|.$$

From Proposition 4, the condition for σ SMC writes

$$\sum_{k,j} (|k\rangle\langle k|)^{\otimes m} \rho (|j\rangle\langle j|)^{\otimes m} = \rho,$$

so (7) must reduce to

$$\rho = \sum_{k,j} p_{kj} |kk \dots k\rangle\langle jj \dots j| \quad (7)$$

for some $p_{kj} \in \mathbb{C}$. It is straightforward to see that a ρ of this form satisfies SSC, since any element in the sum is invariant w.r.t. subsystem permutations. \square

C. On detecting consensus

In the quantum setting, the relation between state and accessible information is stochastic at a fundamental level. In fact, even a “deterministic”, maximal information state yields probabilistic outcomes for certain observables. As we are compelled to use probabilistic notions, consensus can only be inferred from stochastic measurement records, and different types of consensus require different types of measurement statistics.

The σ EC, requiring only equal expectations for a particular observable σ on the different subsystems, is trivial to relate to measurement results; in particular, checking σ EC does not require to monitor correlations between measurement results on different subsystems. Checking RSC requires statistics for a basis of observables for each subsystem; as for σ EC, potential correlations between measurement results on different subsystems play no role. On the other hand, distinguishing SSC from RSC does require to inspect correlations between measurement outcomes at different subsystems – except for the case mentioned in Proposition 3, where SSC can be inferred directly from the special form of the reduced state of each subsystem. A proof of this is provided in Appendix B. For instance, considering the state ρ^B of Example 1, measurements of σ_z on the three subsystems would quickly show that the results on subsystems 2 and 3 are always perfectly correlated, and show no correlation at all with the results on the first subsystem. This difference in correlations rules out ρ^B as a candidate for SSC. The definition of σ SMC is all about correlations between measurement outcomes at different subsystems: the latter must be fully correlated for a particular observable σ .

Positively detecting states in $\mathcal{C}_{\text{SSC}} \setminus \mathcal{C}_{\sigma\text{SMC}}$, however, appears to be less obvious (except through full state tomography). Indeed, a priori it would require to check how permutations affect the full state, including not only classical correlations but also *entanglement* (see Appendix A for a quick review), an intrinsically quantum type of correlation that plays a central role in quantum information theory and its applications [14], [35].

III. QUANTUM EVOLUTIONS FOR CONSENSUS

So far we have been concerned with discussing “static” properties of consensus states. However, the core of the problem is the design of dynamical interactions (or algorithms) that drive the system to consensus. In the following sections, we will establish which dynamics are needed to drive an arbitrary initial state towards a consensus state. In addition to this, as in the classical consensus problems, we shall require the final state to preserve or express some property dependent on the initial state. For example, when classical average consensus is reached, each agent locally contains (“has computed”) the average of the initial state values, which is a global property. In the quantum case as well, a goal when reaching consensus would often be to retrieve, in the final state of any local subsystem, some global information about the initial state.

A. Classical Dynamics and Locality

For classical consensus, the starting point is a first-order integrator dynamics for each individual agent, of the type:

$$x_k(t+1) = x_k(t) + u_k(t) \quad \text{or} \quad \frac{d}{dt} x_k(t) = u_k(t), \quad (8)$$

for $k = 1, 2, \dots, m$. In this paper we focus on the discrete-time case. The inputs $u_k(t)$ for the agents can take different forms, but they are all based on *local information*. A notion of locality is traditionally introduced by specifying a graph $G(V, E)$ whose vertices are the agents $1, 2, \dots, m$ and where an edge $(j, k) \in E$ (unordered pair of vertices) indicates that agents j and k are neighbors. Then for each k , input u_k is restricted to depend only on x_k and on the states x_j of agents j for which $(j, k) \in E$. Mostly, u_k is written as the sum of contributions from different edges, $u_k(t) = \sum_{j:(j,k) \in E} f_{j,k}(x_k(t), x_j(t))$. Directed graphs can be used to model directed information flow, i.e. E contains directed edges (ordered pairs of vertices) such that $(j, k) \in E$ indicates that u_k depends on x_j , but not necessarily u_j on x_k (the latter being governed by another potential edge, $(k, j) \in E$). Weights $w_{(j,k)}$ can be associated to the edges to model their different relative strengths. Besides the *given* asymmetry through edge weights, one usually forbids u_k to explicitly use agent identifiers and apply a different treatment to information coming from or going towards different neighbors. This implies

$$u_k(t) = \sum_{j:(j,k) \in E} w_{(j,k)} f(x_j, x_k), \quad (9)$$

where now f must be independent of j, k . Finally, one may request that the influence of agent j on agent k be exactly equivalent to the reverse influence, of agent k on agent j . Then u_k of the type (9) features symmetric weights, $w_{(j,k)} = w_{(k,j)}$ — leading to an undirected weighted graph — and the antisymmetry property $f(x, y) = -f(y, x)$ for any $x, y \in \mathbb{R}^n$. Such evolution would preserve the average of the state values.

More generally, locality can be defined on the basis of *quasi-local operators*. Instead of considering a graph, we define a set of *neighborhoods* $\mathcal{N}_j \subseteq \{1, \dots, m\}$ for $j = 1, \dots, M$, and a quasi-local operator is one that leaves the states of all subsystems unchanged except those of one neighborhood \mathcal{N}_j . Then a simple dynamics with local coupling

would write

$$x(t+1) = \sum_{j=1}^M V_j(x(t)) \quad (10)$$

where $V_j : \mathbb{R}^{mn} \rightarrow \mathbb{R}^{mn}$ for each j is a quasi-local operator acting on the neighborhood \mathcal{N}_j . Treating all involved agents equivalently can be formulated as requiring that for each j , the quasi-local operator satisfies $PV_j = V_jP$ for all the permutations P that only permute agents of \mathcal{N}_j . The classical consensus algorithm (8),(9) is obtained by taking two-agent neighborhoods only, and identifying each \mathcal{N}_j with an edge of the graph.

B. Quantum Dynamics and Locality

According to Schrödinger's equation, *isolated* quantum systems evolve unitarily [36], [14]. However, unitary dynamics are not enough when we are interested in studying or engineering convergence features for a quantum system. A more general framework that includes (Markovian) open-system evolutions is offered by *quantum channels* [37], [14], that is, linear, completely positive (CP) and trace preserving (TP) maps from density operators to density operators $\mathcal{E} : \mathfrak{D}(\mathcal{H}^m) \rightarrow \mathfrak{D}(\mathcal{H}^m)$. It can be shown that such maps admit an *operator sum representation* (OSR), also known as *Kraus decomposition*:

$$\mathcal{E}(\rho) = \sum_{k=1}^K A_k \rho A_k^\dagger \quad \text{with} \quad \sum_{k=1}^K A_k^\dagger A_k = I \quad (11)$$

where $K \leq (\dim(\mathcal{H}))^2$. The representation is not unique, but all the representations can be obtained as unitary combination of the operators of a given one (see [14, Theorem 8.2]). A CPTP map is said *unital* if $\mathcal{E}(I) = I$. Unital quantum channels can always be represented as given by random unitaries [38]. A channel belongs to this class when it admits an OSR with operators $A_k = \sqrt{p_k} U_k$, with $U_k \in \mathfrak{U}(\mathcal{H}^m)$ and $p_k \geq 0$ such that $\sum_k p_k = 1$:

$$\mathcal{E}(\rho) = \sum_k p_k U_k \rho U_k^\dagger.$$

Such a map can be thought of as a probabilistic mixture of unitary evolutions.

Given a CPTP map \mathcal{E} , we can define its dual map with respect to the Hilbert-Schmidt inner product $\mathcal{E}^\dagger : \mathfrak{B}(\mathcal{H}) \rightarrow \mathfrak{B}(\mathcal{H})$ through the relation:

$$\text{Tr}[A \mathcal{E}(\rho)] = \text{Tr}[\mathcal{E}^\dagger(A) \rho]. \quad (12)$$

This dual map is still linear and completely positive, while the fact that \mathcal{E} is trace preserving implies that \mathcal{E}^\dagger is always unital. Considering the dynamics in the dual picture, i.e. with time-invariant states and maps acting on the observables, is called Heisenberg's picture in the physics literature and provides an equivalent description of quantum system evolution.

We now introduce *locality notions* for the quantum network. Consider the multipartite system introduced in Section II-B: following [25], we say that an operator in $\mathfrak{B}(\mathcal{H})$ is quasi-local if it acts non-trivially only on one neighborhood $\mathcal{N}_j \subseteq \{1, \dots, m\}$:

Definition 5 (Quantum quasi-local operator): An operator V is quasi-local with respect to a set of neighborhoods $\{\mathcal{N}_j, j = 1, 2, \dots, M\}$, if and only if there exists $j \in \{1, 2, \dots, M\}$ such that:

$$V = V_{\mathcal{N}_j} \otimes I_{\overline{\mathcal{N}_j}} \quad (13)$$

where, with a slight abuse of notation, $V_{\mathcal{N}_j}$ accounts for the non trivial action on $\mathcal{H}_{\mathcal{N}_j}$ and $I_{\overline{\mathcal{N}_j}} = \bigotimes_{k \notin \mathcal{N}_j} I_k$.

C. Timing of operations and evolution types

In classical consensus, an important aspect is that the graph (and the related interaction law) can be time-varying. For instance one can assume that all edges are activated for the whole time (*synchronous update*), at the other extreme that they are activated one at a time, or some at each time (*asynchronous update*), according to some predefined time-varying sequence or by random selection of edges. Interestingly, convergence properties for all these cases can be linked to the connectedness of the ‘‘average graph’’ [13].

In the quantum case also this distinction can be made. The elementary dynamical interaction that we consider, replacing ‘‘one edge’’ of the classical case, is a CPTP map involving one neighborhood only:

$$\mathcal{E}_{\mathcal{N}_j}(\rho) = \sum_k p_k V_k(t) \rho V_k^\dagger(t), \quad (14)$$

where all the $V_k(t) \in \mathfrak{U}(\mathcal{H}^m)$ are quasi-local with respect to the neighborhood \mathcal{N}_j . One of the reasons for focusing on this class of evolutions stems directly from applications: methods for implementing unitary evolutions, as well as related unital channels with the aid of some ancillary systems, are available in a number of diverse experimental settings. On the other hand, constructing arbitrary quantum channels is a more challenging task [39], and can be generally done with good approximation only in the limit of fast control and/or short time scales [40]. The building block (14) can lead to different evolutions for the whole system, depending on neighborhood selection:

- *Random single interaction:* at each time t one neighborhood $\mathcal{N}_{j(t)}$ is selected at random, $j(t)$ being a single-valued random variable onto the neighborhood index set.
- *Cyclic single interaction:* at each time t one neighborhood $\mathcal{N}_{j(t)}$ is selected deterministically, for example periodically cycling between the available j .
- *Random or cyclic asynchronous interactions:* similar to the previous options, but a subset of several neighborhoods is selected at each time t . We can request the selected neighborhoods to be disjoint or not. *This choice has an effect for implementation, but not for convergence properties of our algorithm*, so we will not consider it further.
- *Synchronous interaction:* all the available interactions are activated at each time, weighted by some $q_j \geq 0$ with $\sum_j q_j = 1$ in order to maintain a valid trace-preserving map:

$$\mathcal{E}(\rho) = \sum_j q_j \mathcal{E}_{\mathcal{N}_j}(\rho). \quad (15)$$

- *Expected evolution:* we study the evolution in expectation of the random interaction protocol which selects neighborhood \mathcal{N}_j with probability q_j at each t . Remarkably, the evolution to ρ_{t+1} given ρ_t then follows the same law (15) as the synchronous case. Note that convergence of the expected evolution to consensus does not guarantee (at all) that a(ny) single evolution, determined by a realization of the random process $\{j(t)\}_{t \geq 0}$, would converge to consensus. Nevertheless, the statistics of any measurements performed at any time on the system will be exactly the same for (15) as for the associated random evolution. In this sense, convergence in expectation is indistinguishable from trajectory-wise convergence.

The last two cases involve a time-independent map. Another time-independent map is obtained if we consider cyclic interactions of period T and we focus on the state at the end of every cycle:

$$\rho_{t+T} = \mathcal{E}_C(\rho_t) = \mathcal{E}_{\mathcal{N}_T} \circ \dots \circ \mathcal{E}_{\mathcal{N}_1}(\rho_t). \quad (16)$$

The consensus goal can now be specified formally.

Let $d(\rho_a, \mathcal{C}) = \inf_{\rho \in \mathcal{C}} \|\rho_a - \rho\|$, where $\mathcal{C} \subset \mathfrak{D}(\mathcal{H})$ and $\|\cdot\|$ is any p -norm on $\mathfrak{B}(\mathcal{H})$. Given a sequence of channels $\{\mathcal{E}_t(\cdot)\}_{t=0}^\infty$, define $\hat{\mathcal{E}}_t(\rho_0) = \rho_t = \mathcal{E}_t \circ \mathcal{E}_{t-1} \circ \dots \circ \mathcal{E}_1(\rho_0)$.

Definition 6 (Asymptotic Consensus): A sequence of channels $\{\mathcal{E}_t(\cdot)\}_{t=0}^\infty$, is said to *asymptotically achieve σEC* if

$$\lim_{t \rightarrow \infty} d(\hat{\mathcal{E}}_t(\rho_0), \mathcal{C}_{\sigma EC}) = 0, \quad (17)$$

for all initial states ρ_0 .

The same definition holds for RSC, SSC, and σSMC by substituting the corresponding state sets in (17).

Definition 7 (Asymptotic Average Consensus): We say that the sequence of channels $\{\mathcal{E}_t(\cdot)\}_{t=0}^\infty$ asymptotically achieves *S -average σEC* for some $S \in \mathfrak{H}(\mathcal{H}^m)$ if it asymptotically achieves σEC and for all ρ_0 , it holds:

$$\begin{aligned} \lim_{t \rightarrow \infty} \text{Tr}(\sigma \bar{\rho}_\ell(t)) &= \lim_{t \rightarrow \infty} \text{Tr}(\sigma^{(\ell)} \rho(t)) = \lim_{t \rightarrow \infty} \text{Tr}(S \rho(t)) \\ &= \text{Tr}(S \rho_0) \end{aligned} \quad (18)$$

for all $\ell \in \{1, \dots, m\}$. The same definition holds for σSMC . We say that the sequence of channels $\{\mathcal{E}_t(\cdot)\}_{t=0}^\infty$ asymptotically achieves *S -average RSC (resp. SSC)* if it asymptotically achieves RSC (resp. SSC) and for $S \in \mathfrak{H}(\mathcal{H}^m)$ there exists a $\sigma \in \mathfrak{H}(\mathcal{H})$ such that (18) holds for all ρ_0 .

By expressing the action of quantum channels in the dual (Heisenberg) picture, it is possible to obtain a clear characterization of the dynamics that satisfy (18).

Proposition 6: Consider a sequence of CPTP channels $\{\mathcal{E}_t(\cdot)\}_{t=0}^\infty$, and call $\hat{\mathcal{E}}_t = \mathcal{E}_t \circ \mathcal{E}_{t-1} \circ \dots \circ \mathcal{E}_1$. The associated dynamics satisfies (18) if and only if

$$S = \lim_{t \rightarrow \infty} \hat{\mathcal{E}}_t^\dagger(S) \quad \text{and} \quad \lim_{t \rightarrow \infty} \hat{\mathcal{E}}_t^\dagger(\sigma^{(\ell)}) = S \quad (19)$$

for $\ell = 1, 2, \dots, m$, where $\hat{\mathcal{E}}_t^\dagger = \mathcal{E}_1^\dagger \circ \mathcal{E}_2^\dagger \circ \dots \circ \mathcal{E}_t^\dagger$.

Proof: The conditions (19) clearly imply (18). On the other hand, if (18) holds for all ρ_0 , it is easy to obtain (19) by duality, taking the limit inside the trace functional. ■

The first of the equalities in (19) holds in particular for the natural situation where $\mathcal{E}_t^\dagger(S) = S$ for all t .

IV. A GOSSIP ALGORITHM FOR QUANTUM CONSENSUS

We now propose actual interactions that drive the quantum network to average consensus. As a building block, we focus on the interaction between two subsystems while the others remain unchanged; all neighborhood-activation options build on this elementary case, as explained above.

A. Another viewpoint on the Classical Gossip Algorithm

The standard linear consensus algorithm corresponds to (8),(9) with $f(x, y) = \alpha(x - y)$. Its form with a single interaction activated at any time — also called *gossip algorithm* — is usually described as follows [41]. At each iteration, a single edge (j, k) is selected from the set $E(t)$ of available edges at that time. The associated agents move towards each other / their mean value, according to:

$$\begin{aligned} x_j(t+1) &= x_j(t) + \alpha(x_k(t) - x_j(t)) \\ &= (1 - \beta)x_j(t) + \beta \frac{x_j(t) + x_k(t)}{2} \\ x_k(t+1) &= x_k(t) + \alpha(x_j(t) - x_k(t)) \\ &= (1 - \beta)x_k(t) + \beta \frac{x_j(t) + x_k(t)}{2} \\ x_\ell(t+1) &= x_\ell(t) \quad \text{for all } \ell \notin \{j, k\}, \end{aligned} \quad (20)$$

where $\alpha \in (0, 1)$ to have meaningful results³, and $\beta = 2\alpha$. An alternative viewpoint on this behavior is that the interacting agents take a weighted average between two discrete operations: [keep your state] and [swap your state]; namely

$$\begin{aligned} (x_j(t+1), x_k(t+1)) &= (1 - \alpha)(x_j(t), x_k(t)) \\ &\quad + \alpha(x_k(t), x_j(t)) \\ x_\ell(t+1) &= x_\ell(t) \quad \text{for all } \ell \notin \{j, k\}. \end{aligned} \quad (21)$$

This latter viewpoint turns out to have a natural quantum counterpart. Working with neighborhoods, one could also apply multi-agent permutations, e.g.

$$\begin{aligned} (x_j, x_k, x_l)_{t+1} &= (1 - \alpha - \beta)(x_j, x_k, x_l)_t + \alpha(x_k, x_l, x_j)_t \\ &\quad + \beta(x_l, x_j, x_k)_t. \end{aligned}$$

The following result (see e.g. [41]) characterizes convergence to consensus with the gossip algorithm. While it is a known result, we nonetheless provide a proof that will be useful to our aim, i.e. proving the convergence of the quantum gossip algorithm, and makes our presentation more self-contained.

Proposition 7: Consider $G(V, E)$ an undirected graph that is connected, i.e. for any pair of vertices $a, b \in V$, there exists a sequence of vertices $v_0 = a, v_1, v_2, \dots, v_{n-1}, v_n = b$ such that $(v_{k-1}, v_k) \in E$ for all $k = 0, 1, \dots, n$. If one step of the classical gossip algorithm (20) is applied at each time, selecting the updated edge by cyclically running through all the edges of $G(V, E)$, then the system exponentially converges to average consensus. Moreover, if the updated edge (j, k) is selected randomly according to a fixed probability distribution $\{q_{j,k}\}$, with all $q_{j,k} > 0$, then asymptotic average consensus is ensured with probability one, in the sense that: for any $\delta, \varepsilon > 0$, there exists a time $T > 0$ such that

$$\mathbb{P}[\|x_k(T) - \bar{x}\|^2 > \varepsilon \|x_k(0) - \bar{x}\|^2] < \delta,$$

³That is, the new states are an interpolation and not extrapolation between $x_j(t)$ and $x_k(t)$.

where \mathbb{P} denotes the probability measure induced by the randomization, $\|x\|^2 = \sum_k x_k^T x_k$ and $\bar{x} = \frac{1}{m} \sum_k x_k(t) = \sum_k x_k(0)$ for any choice of the edges.

Proof: We denote $x^T x = \|x\|^2$ for short and $\#E$ the number of edges in $G(V, E)$. At any step of the gossip algorithm, $W := \frac{1}{2m} \sum_{k,j} \|x_k - x_j\|^2 = \sum_k \|x_k - \bar{x}\|^2$ can only remain unchanged (if the two nodes of the selected edge have the same value) or decrease (as soon as an edge with different node values is selected). A Lyapunov argument on W then shows that the system must asymptotically converge to average consensus when the edges of a connected graph are selected in a cyclic way. Since the map associated to one full cycle of edge selections is linear and time-invariant, this convergence is exponential. For such convergence to be possible, there must exist some $\lambda > 0$ and integer $M > 0$ such that $W(T) \leq W(0)\lambda$ if the edge choice between $t = 0$ and $t = T = M\#E$ corresponds to M cycles of gossip iteration. When edges are selected randomly, any particular sequence of b consecutive edge selections has a probability greater than $\bar{q}^b > 0$ to appear at least once during any time interval of length at least b , where $\bar{q} = \min_{(j,k) \in E} q_{j,k}$. In particular, if we target $W(T) < \varepsilon W(0) = \lambda^r W(0)$, we can say that there is a probability at least $\bar{q}^{rM\#E}$ to select r times a succession of M cyclic interactions between $t = t_0$ and $t = t_0 + rM\#E$. If this happens once, any preceding or following edge choice can only improve W (because of our first statement in this proof). We conclude by noting that over a time interval $brM\#E$, there is then a probability $< (1 - \bar{q}^{rM\#E})^b$ to have never selected r times a succession of M cyclic interactions, and thus potentially miss $W(T) < \varepsilon W(0)$; the probability that this happens can be made arbitrarily small by taking b (thus T) sufficiently large. \square

B. Quantum Gossip Interactions

Let us introduce a way to implement gossip-type interactions in a fully quantum way. In a controlled quantum network, one can typically engineer unitary transformations that implement the ‘‘identity’’ evolution and the swapping of two neighboring subsystem states; let us denote the latter operator by $U_{(j,k)}$ for swapping subsystems j and k . By conditionally associating these two operations to orthogonal states $|\xi_I\rangle$ and $|\xi_S\rangle$ of an ancillary quantum two-level system and starting that auxiliary system in the state $\rho_\xi = (1 - \alpha)|\xi_I\rangle\langle\xi_I| + \alpha|\xi_S\rangle\langle\xi_S|$, the joint state would evolve as:

$$\rho \otimes \rho_\xi \rightarrow (1 - \alpha)\rho \otimes |\xi_I\rangle\langle\xi_I| + \alpha U_{(j,k)}\rho U_{(j,k)}^\dagger \otimes |\xi_S\rangle\langle\xi_S|.$$

The evolution of the composite system is thus described by a single unitary transformation.⁴ Taking the partial trace over the ancillary system, we obtain as evolution for the quantum network a quantum gossip interaction implementing the quantum channel:

$$\rho(t+1) = \mathcal{E}_{j,k}(\rho(t)) = (1 - \alpha)\rho(t) + \alpha U_{(j,k)}\rho(t)U_{(j,k)}^\dagger, \quad (22)$$

⁴The unitary transformation being given by $I \otimes |\xi_I\rangle\langle\xi_I| + U_{(j,k)} \otimes |\xi_S\rangle\langle\xi_S|$.

with $\alpha \in (0, 1)$. The optimal quasi-local mixing is obtained with $\alpha = 1/2$.

To develop our analysis, it will be convenient to introduce the *graph \mathcal{G} associated to the multipartite system*: its nodes $1, \dots, m$ correspond to the ‘‘physical’’ subsystems, the edge (j, k) is included if the subsystems j and k have a non-zero probability to interact.

C. Convergence to Consensus

We study convergence under three types of gossip dynamics: cyclic interaction, expectation of random interaction, and trajectory-wise for the random interaction. In all these cases, quantum gossip can be described by unital CPTP maps. We begin by recalling a characterization of the fixed points of such maps (see e.g. [19]).

Proposition 8: Let $\{V_i\}_{i=1}^K$ the Kraus decomposition of a unital CP map $\mathcal{E}(\cdot)$ and define:

$$\mathcal{A}_\mathcal{E} = \{X \in \mathfrak{B}(\mathcal{H}^m) \mid [X, V_i] = 0 \ \forall i = 1, \dots, K\}. \quad (23)$$

Then $\bar{X} \in \mathfrak{B}(\mathcal{H}^m)$ is a fixed point of \mathcal{E} , i.e. $\mathcal{E}(\bar{X}) = \bar{X}$, if and only if $\bar{X} \in \mathcal{A}_\mathcal{E}$. \square

This helps determine the set of fixed points for the CP maps of interest in quantum gossip.

Lemma 1: Let $U_{(j,k)}$ denote the pairwise swap operation of subsystems (j, k) on \mathcal{H}^m . If the graph \mathcal{G} associated to the system is connected, then the set of fixed points of any CP unital map of the form

$$\mathcal{E}(X) = q_0 X + \sum_{(j,k) \in E} q_{j,k} U_{(j,k)} X U_{(j,k)}^\dagger, \quad (24)$$

$$\text{with } q_0 + \sum q_{j,k} = 1, \quad q_0, \{q_{j,k}\} > 0$$

coincides with the set of permutation-invariant operators.

Proof: According to Proposition 8 above, the fixed points are the X satisfying $XU_{(j,k)} = U_{(j,k)}X$, or equivalently $U_{(j,k)}^\dagger XU_{(j,k)} = X$. The latter expresses that X is invariant with respect to pairwise swaps on all the graph edges. It is well known that sequences of pairwise swaps on the edges of a connected graph generate the full set of permutations on the set of nodes, and so we get the conclusion. \square

The following lemma shows how the contribution of the identity, i.e. the trivial permutation, in the CP map plays a crucial role in the proof of convergence.

Lemma 2: If a CP map \mathcal{E} admits an OSR with a term $V_1 = \sqrt{\alpha}I$ with $\alpha > 0$, then viewing it as a linear map on $\mathfrak{B}(\mathcal{H}^m)$ its only modulus-one eigenvalue can be one.

Proof: If \mathcal{E} is a CPTP map it is a contraction in trace norm [14], [42], so its eigenvalues λ_k belong to the closed unit disk. By virtue of the Kraus-Stinespring representation theorem (see e.g. [37]), also $\mathcal{F} = \frac{1}{1-\alpha}(\mathcal{E} - \alpha I)$ is CPTP and thus has eigenvalues μ_k in the closed unit disk. Therefore the eigenvalues $\lambda_k = (1 - \alpha)\mu_k + \alpha$ of $\mathcal{E} = (1 - \alpha)\mathcal{F} + \alpha I$ in fact belong to the circle of radius $(1 - \alpha)$ centered at α , which is strictly inside the unit circle except for a tangency point at $1 \in \mathbb{C}$, see Fig. 1. \square

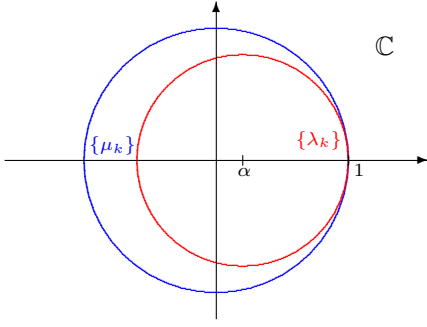


Fig. 1. Delimitation of the (closed) domains for the eigenvalues $\{\mu_k\}$ of \mathcal{F} (blue) and $\{\lambda_k\}$ of \mathcal{E} (red) [color online].

In other words, Lemma 2 excludes eigenvalues of unit norm different from +1, which are the ones that would cause limit cycles.

By combining the above properties, we get the following convergence result for quantum gossip. It shows that S -average SSC can be attained for global operators that are the permutation-invariant average of local ones; this is similar to classical gossip, where distributed computation of the average of individual states actually gives access to the value of any linear permutation-invariant function of these states.

Theorem 2: If the graph associated to possible interactions is connected, then the quantum gossip algorithm (22) ensures global convergence towards SSC:

- deterministically, when the edges on which a gossip interaction occurs at a given time are selected by periodically cycling, in any predefined way, through the set of edges;
- in expectation, when the edges on which a gossip interaction occurs at a given time are selected randomly from a fixed probability distribution $\{q_{j,k} > 0 \mid \sum_{(j,k) \in E} q_{j,k} = 1\}$;
- with probability one on any trajectory, with the same edge-selection strategy of the previous point. Explicitly, there exists a state $\rho_* \in \mathcal{C}_{SSC}$ for which for any $\delta, \varepsilon > 0$, there exists a time $T > 0$ such that

$$\mathbb{P}[\text{Tr}((\rho(T) - \rho_*)^2) > \varepsilon] < \delta.$$

In any of the cases above, the state towards which the system converges is:

$$\rho_* = \frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi \rho_0 U_\pi^\dagger. \quad (25)$$

Furthermore, S -average SSC is attained if and only if $S \in \mathfrak{H}(\mathcal{H}^{\otimes m})$ can be written, for some $\sigma \in \mathfrak{H}(\mathcal{H})$, in the form:

$$S = \frac{1}{m} \sum_i^m \sigma^{(i)}. \quad (26)$$

Proof: First notice that all the operators in the OSR of the map (24) are self-adjoint. This implies that permutation-invariant observables S are fixed points for the associated dual map, and hence for the gossip iteration associated to any edge (j, k) and $\forall \rho$:

$$U_{(j,k)} S U_{(j,k)}^\dagger = S \Rightarrow \text{Tr}[\mathcal{E}_{j,k}(\rho) S] = \text{Tr}[\rho \mathcal{E}_{j,k}^\dagger(S)] = \text{Tr}[\rho S] \quad (27)$$

For the *cyclic evolution* map \mathcal{E}_C , we notice that all the simple two-subsystem swaps are still present with a weight different from zero in the OSR of the cyclic map (16), thanks to the presence of the identity in the OSR of each gossip interaction step. Therefore by Lemma 1 the fixed points are the permutation-invariant operators. Now consider the dynamics associated to \mathcal{E}_C as a linear, time-invariant map acting on the subspace of hermitian matrices. From Lemma 2 and the fact that the time-invariant linear map leaves $\mathfrak{D}(\mathcal{H}^m)$ invariant (excluding unstable Jordan blocks), we have that all the *modes* of the LTI system are asymptotically stable except those corresponding to the fixed-point set, namely the permutation-invariant set: every initial state converges to a fixed point ρ_∞ in this set. Thus the SSC set is globally asymptotically stable, and in fact exponentially stable since the map is linear. Let us now prove that ρ_∞ has the form (25). For all *permutation invariant* X , from (27) we have that:

$$\text{Tr}[X \mathcal{E}_C(\rho_0)] = \text{Tr}[X \rho_0] \quad \forall t. \quad (28)$$

Combining the latter with the fact that ρ_∞ is permutation-invariant, that the set of all permutations is self-adjoint, and using (3), we get for arbitrary $Q \in \mathfrak{H}(\mathcal{H}^m)$:

$$\begin{aligned} \text{Tr}[Q \rho_\infty] &= \text{Tr}\left[Q \frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi \rho_\infty U_\pi^\dagger\right] \\ &= \text{Tr}\left[\frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi Q U_\pi^\dagger \rho_\infty\right] \\ &= \text{Tr}\left[\frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi Q U_\pi^\dagger \rho_0\right] \\ &= \text{Tr}\left[\frac{1}{m!} \sum_{\pi \in \mathfrak{P}} Q U_\pi \rho_0 U_\pi^\dagger\right]. \end{aligned}$$

This implies that indeed $\rho_\infty = \rho_*$ as described in the statement.

For the *expectation of random evolution*, the CPTP map \mathcal{E} is exactly of the form of Lemma 1 and the same reasoning can be repeated.

For the *random trajectory evolution*, we repeat a proof similar to that of Proposition 7. Since \mathcal{E} for a single interaction is linear, *self-adjoint*, with eigenvalues in the closed unit disk, it is a contraction for the Frobenius norm distance $\text{Tr}((\rho_A - \rho_B)^2)$ between any two states $\rho_A, \rho_B \in \mathfrak{D}(\mathcal{H}^m)$. Indeed, \mathcal{E} has non-increasing orthonormal modes, so by writing any operator $X \in \mathfrak{H}(\mathcal{H}^m)$ in the modal basis we directly get $\text{Tr}(\mathcal{E}(X)^\dagger \mathcal{E}(X)) \leq \text{Tr}(X^\dagger X)$; taking $X = \rho_A - \rho_B$ yields the contraction. This is exactly analogous to the non-increasing Euclidean norm $x^T x = \|x\|^2$ under a classical consensus interaction with an *undirected* graph, and the related contraction of $\|x_A - x_B\|^2$. Now taking in particular $\rho_A = \rho$ and $\rho_B = \rho_*$, we get that the Frobenius distance from ρ to ρ_* can never increase. Moreover, by transitivity of the permutation operators, $\frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi \rho U_\pi^\dagger = \frac{1}{m!} \sum_{\pi \in \mathfrak{P}} U_\pi \rho_0 U_\pi^\dagger = \rho_*$ for any ρ along the trajectory of the gossip algorithm. Now given the convergence under cyclic evolution, there must exist some $\lambda < 1$ and integer $M > 0$ such that

$$\text{Tr}((\mathcal{E}_C^M(\rho) - \rho_*)^2) \leq \lambda \text{Tr}((\rho - \rho_*)^2)$$

for any ρ for which $\frac{1}{m!} \sum_{\pi \in \mathfrak{S}^m} U_\pi \rho U_\pi^\dagger = \rho_*$. The proof then concludes along the same lines as Proposition 7, namely the probability to obtain an edge sequence which includes successions of M cyclic evolutions a sufficiently large number of times to have ε -convergence, gets arbitrarily close to 1 if we wait long enough.

Finally let us prove that we attain S -average consensus if and only if S can be decomposed as in (26). We know from the first part of the proof that all permutation-invariant observables S are fixed points for the associated dual map \mathcal{E}_t^\dagger . Then according to Proposition 6 we have S -average consensus if and only if there exists a local observable σ such that:

$$\lim_{t \rightarrow \infty} \hat{\mathcal{E}}_t^\dagger(\sigma^{(\ell)}) = S \quad (29)$$

for $\ell = 1, 2, \dots, m$. Because of (27) and (25), by duality we have that for every local operator $\sigma^{(\ell)}$:

$$\lim_{t \rightarrow \infty} \hat{\mathcal{E}}_t^\dagger(\sigma^{(\ell)}) = \frac{1}{m!} \sum_{\pi \in \mathfrak{S}^m} U_\pi^\dagger \sigma^{(\ell)} U_\pi = \frac{1}{m} \sum_{i=1}^m \sigma^{(i)}. \quad (30)$$

Therefore, we can achieve S -average consensus if and only if S is a permutation invariant operator that can be decomposed as in (26). \square

Remark: This shows that the mean value of a (global) observable $S = \frac{1}{m} \sum_{\ell} \sigma^{(\ell)}$, with arbitrary σ , can be asymptotically retrieved from the state of any single subsystem after having applied one of the quantum gossip algorithms.

On the other hand, unlike for classical consensus, there are permutation-invariant operators that do not attain S -average consensus, because they cannot be written in the form (26). This is the case among others if S is orthogonal to the linear span of all the local observables. For instance if $\tilde{S} = \sigma_z^{\otimes m}$, given the orthogonal basis $\{\sigma_k\}_{k=0,x,y,z}$ for $\mathfrak{B}(\mathcal{H})$, we have:

$$\text{Tr}[\tilde{S} \sigma_k^{(\ell)}] = 0 \quad \forall k \in \{0, x, y, z\} \text{ and } \forall \ell \in \{1, \dots, m\}.$$

Therefore \tilde{S} cannot be written in the form (26), hence although \tilde{S} is conserved by the gossip algorithm, the latter cannot lead to \tilde{S} -average consensus in the sense of Definition 7.

As already mentioned, the convergence speed for the random case can be quite low, and a faster map would be obtained by effectively taking a mixture of all possible updates at each time. This can be attained by suitably selecting edges through an auxiliary quantum system, acting as an independent quantum ‘‘coin’’ (in the jargon of quantum random walks) at each time. This would represent a fully quantum implementation of a *synchronous consensus update*.

D. Classical equivalent to observable consensus dynamics

We next show how the quantum gossip algorithm (22) in fact implements in a quantum fashion the classical gossip as we restrict to σ EC. According to Definition 1, a quantum state ρ belongs to $\mathcal{C}_{\sigma\text{EC}}$ if:

$$\text{Tr}[\sigma^{(1)} \rho] = \dots = \text{Tr}[\sigma^{(m)} \rho]. \quad (31)$$

In view of this, it seems reasonable to attempt a convergence study of the algorithm (22) directly in terms of the evolution

of the expectation values of the $\sigma^{(\ell)}$ operators. This is not possible for arbitrary quantum evolutions, since a quantum state is far from fully specified by a *single* set of commuting observable expectations, and different states with the same expectation may lead to very different evolutions. However, our quantum gossip algorithm remarkably allows us to write a model for the average dynamics of the $\sigma^{(\ell)}$ in closed form. More precisely, let us define $z_\ell(t) := \text{Tr}[\mathcal{E}^t(\rho_0) \sigma^{(\ell)}] = \text{Tr}[\rho_t \sigma^{(\ell)}]$. Note that for one subsystem swap $U_{(j,k)}$, we have:

$$\text{Tr}[\sigma^{(\ell)} U_{(j,k)} \rho U_{(j,k)}^\dagger] = \begin{cases} z_\ell & \text{if } \ell \notin \{j, k\} \\ z_k & \text{if } \ell = j \\ z_j & \text{if } \ell = k. \end{cases} \quad (32)$$

According to (32) and (22), the random gossip algorithm update yields, with probability $q_{j,k}$, i.e. when the edge (j, k) is selected:

$$(z_j(t+1), z_k(t+1)) = (1 - \alpha)(z_j(t), z_k(t)) + \alpha(z_k(t), z_j(t)) \\ z_\ell(t+1) = z_\ell(t) \quad \text{for all } \ell \notin \{j, k\}.$$

This last expression has exactly the same form as the classical gossip algorithm (21). Therefore, Proposition 7 readily implies:

Corollary 1: Under all the various edge selection strategies for quantum consensus algorithm (22), the $z_\ell(t)$, $\ell = 1, 2, \dots, m$ asymptotically converge towards the unique configuration:

$$\lim_{t \rightarrow \infty} z_\ell(t) = \frac{1}{m} \sum_{k=1}^m z_k(0) \quad \text{for all } \ell \in \{1, 2, \dots, m\}.$$

\square

We remark that this only proves average σ -Expectation Consensus of the quantum gossip algorithm, while our previous Theorem 2 shows that the algorithm in fact ensures the stronger average *Symmetric State Consensus*.

E. Gossip algorithm example

In this section we briefly discuss the evolution induced by random quantum gossip interactions (22) on a four-qubit network whose associated graph is a path⁵. We observe its convergence toward average σ EC, average RSC and average SSC. In particular we consider as a ‘‘target’’ global observable:

$$S = \frac{1}{4} \left(\sigma_z^{(1)} + \sigma_z^{(2)} + \sigma_z^{(3)} + \sigma_z^{(4)} \right). \quad (33)$$

Let the initial state be:

$$\rho = |1, 0, 1, 0\rangle \langle 1, 0, 1, 0|, \quad (34)$$

which is pure, and does not satisfy any of the consensus definitions provided in Section II.

⁵I.e. the available neighborhoods, labeling the subsystems as $\{1, 2, 3, 4\}$, are $\{1, 2\}$, $\{2, 3\}$ and $\{3, 4\}$.

By Theorem 2 we have that the state asymptotically converges to:

$$\begin{aligned} \rho_\infty &= \lim_{t \rightarrow \infty} \rho(t) = \frac{1}{3!} \sum_{\pi \in \mathfrak{S}} U_\pi \rho_0 U_\pi^\dagger \\ &= \frac{1}{6} (|1, 1, 0, 0\rangle\langle 1, 1, 0, 0| + |1, 0, 1, 0\rangle\langle 1, 0, 1, 0| \\ &\quad + |1, 0, 0, 1\rangle\langle 1, 0, 0, 1| + |0, 1, 1, 0\rangle\langle 0, 1, 1, 0| \\ &\quad + |0, 1, 0, 1\rangle\langle 0, 1, 0, 1| + |0, 0, 1, 1\rangle\langle 0, 0, 1, 1|). \end{aligned} \quad (35)$$

This expression is clearly invariant under all the subsystem permutations, i.e. ρ_∞ is in SSC, and therefore also in RSC and σ EC for all σ . The expectation value of S is preserved at any step, and by Theorem 2 the algorithm drives the system to S -average consensus, with $\sigma = \sigma_z$.

However, ρ_∞ is not in σ SMC for any $\sigma \neq \alpha I$. Indeed, according to Proposition 4, ρ_∞ is in σ SMC if and only if $\text{Tr}[\rho_\infty \Pi_{sym}] = 1$. Now let $\{\Pi_i\}_{i=1}^6$ denote the orthonormal rank-one projectors in (35) and define the orthonormal projector $\bar{\Pi} = \sum_i \Pi_i$, such that $\rho_\infty = \frac{1}{6} \sum_{i=1}^6 \Pi_i = \frac{1}{6} \bar{\Pi}$. We then get

$$\text{Tr}[\rho_\infty \Pi_{sym}] = \frac{1}{6} \text{Tr}[\sum_{i=1}^6 \Pi_i \Pi_{sym}] = \frac{1}{6} \text{Tr}[\Pi_{sym} \bar{\Pi}]. \quad (36)$$

This last expression is equal to 1 if and only if $\text{Tr}[\Pi_{sym} \bar{\Pi}] = 6$. However, excluding the trivial case $\sigma = \alpha I$, for qubit networks Π_{sym} is always a two dimensional projector, so $\text{Tr}[\Pi_{sym} \bar{\Pi}] \leq 2$. Hence ρ_∞ cannot be in σ SMC for any non-trivial σ .

Figure 2 shows the evolution of the expectation values of the local and of the global observables related to σ_z as the iterations proceed for one run. The edges are selected at random with uniform probability, and the mixing parameter α is taken to be $1/2$. With this particular choice, the reduced density operators of two subsystems that have just interacted are equal; this explains why a maximum of three points are visible on the graph at any time. The plot shows that asymptotically the expectation of the local observables σ_z tend to the expectation value of the global observable S , while the expectation value of S is preserved at each step.

V. CONCLUSIONS AND RESEARCH DIRECTIONS

In this paper we develop a general framework for posing and studying consensus problems in the quantum domain. In particular we provide various operationally-motivated generalizations of a ‘‘consensus state’’ to quantum systems – namely σ -expectation consensus, reduced state consensus, symmetric state consensus, and single σ -measurement consensus – and establish their hierarchy. We highlight at each step the symmetry considerations underlying the results, making explicit connection with the usual multi-agent consensus problem. The developments could be adapted in particular to obtain a ‘‘consensus on probabilities’’ framework for classical systems. With respect to the existing work on non-commutative consensus [34], our approach follows the analogy with the classical setting as closely as possible, maintaining an operational viewpoint and working with a multipartite system

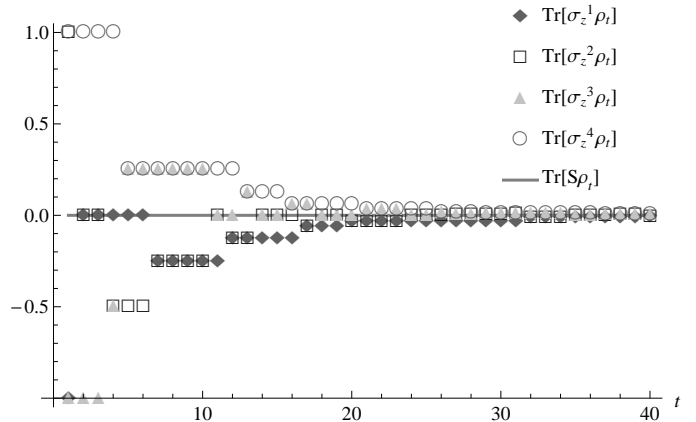


Fig. 2. Evolution toward σ -Expectation Consensus for a four-qubit network arranged in a path graph.

(a quantum network). We propose and analyze a quantum gossip-type algorithm that asymptotically prepares symmetric-state consensus states while preserving the expectation of *any permutation invariant observable*.

A number of questions remain open. Among these, we believe that it would be particularly interesting to further explore the link between single σ -measurement consensus states and entangled states, and to determine if, and under which conditions, it is possible to achieve this type of consensus with a distributed algorithm. This could potentially lead to a class of algorithms that prepare entangled states in a robust and distributed way. Another interesting point is to assess the potential of devising continuous-time quantum consensus algorithms. This could build on some sort of ‘‘continuous swapping’’ Hamiltonian dynamics and lead to connections with physically relevant many-body Hamiltonians and dynamics.

Lastly, let us remark that in this paper we proposed a quantum algorithm in which the gossip-type interactions are selected in a classical way. The potential advantage of a fully quantum implementation, along with its connection to quantum random walks and Markov chain mixing properties [17], [18], is definitely worth further investigation.

APPENDIX

A. Description of quantum systems and notations

1) *Quantum systems basics*: This paper considers finite-dimensional quantum systems. Their mathematical description starts by considering a finite dimensional complex Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$. The (Dirac’s) notation $|\psi\rangle$ denotes an element of \mathcal{H} (called a *ket*), while $\langle\psi| = |\psi\rangle^\dagger$ is used for its dual (a *bra*), and $\langle\psi|\varphi\rangle$ for the associated inner product. We denote the set of linear operators on \mathcal{H} by $\mathfrak{B}(\mathcal{H})$. The adjoint operator $X^\dagger \in \mathfrak{B}(\mathcal{H})$ of an operator $X \in \mathfrak{B}(\mathcal{H})$ is the unique operator that satisfies $(X|\psi\rangle)^\dagger |\chi\rangle = \langle\psi| (X^\dagger |\chi\rangle)$ for all $|\psi\rangle, |\chi\rangle \in \mathcal{H}$. We then denote $\mathfrak{H}(\mathcal{H})$ the subset of $\mathfrak{B}(\mathcal{H})$ of self-adjoint operators, and $\mathfrak{U}(\mathcal{H}) \subset \mathfrak{B}(\mathcal{H})$ the subset of unitary operators. The natural inner product in $\mathfrak{B}(\mathcal{H})$ is the Hilbert-Schmidt product $\langle X, Y \rangle = \text{Tr}(X^\dagger Y)$, where Tr is the usual trace

functional (which is canonically defined in a finite dimensional setting). We denote by I the identity operator. Working in a finite dimensional setting, we often consider vectors and operators as represented by complex matrices of suitable dimensions: $|\psi\rangle \in \mathcal{H} \simeq \mathbb{C}^d$ are represented by column vectors, so $\langle\phi| \in \mathcal{H}^\dagger \simeq \mathbb{C}^d$ are row vectors; $X \in \mathfrak{B}(\mathcal{H}) \simeq \mathbb{C}^{d \times d}$ are $d \times d$ complex matrices, the adjoint X^\dagger is the transpose conjugate of X , self-adjoint and unitary properties carry over to the associated matrices.

In statistical quantum theory, the state of a quantum system is represented by a *density operator* ρ , that is any self-adjoint, positive semi-definite operator with trace one. We denote the convex set of these operators (the state space) by $\mathfrak{D}(\mathcal{H})$. The extreme points of this set, namely the rank-one operators $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \mathcal{H}$ and $\langle\psi|\psi\rangle = 1$, are called *pure states*.

A *projective* (or von Neumann) observation, or measurement, of a quantum system is characterized by a so-called *observable*, that is a self-adjoint operator $\sigma \in \mathfrak{H}(\mathcal{H})$, see e.g. [36]. Its spectral decomposition $\sigma = \sum_j s_j \Pi_j$ determines the possible outcomes $\{s_j\}$ of the measurement, and the projectors Π_j determine the associated state of the quantum system after the stochastic measurement: having state ρ before the measurement, the latter's outcome will be s_j with probability $\mathbb{P}_\rho(\Pi_j) = \text{Tr}(\Pi_j \rho) =: p_j$; and if the j -th outcome is measured, then the state after the measurement is $\rho|_j = \Pi_j \rho \Pi_j / p_j$. The probability to observe s'_k in a subsequent measurement of $\sigma' = \sum_k s'_k \Pi'_k$, where the Π'_k do not necessarily commute with the Π_j , is then:

$$\mathbb{P}_{\rho|_j}(\Pi'_k) = \text{Tr}(\Pi'_k \Pi_j \rho \Pi_j) / p_j.$$

From this it follows that the probability of observing the *ordered* sequence of two events first s_j , then s'_k , given the initial ρ , is

$$\mathbb{P}_\rho(\Pi_j, \Pi'_k) = \text{Tr}(\Pi'_k \Pi_j \rho \Pi_j).$$

If Π_j and Π'_k do not commute, a different ordering in a sequence of measurements can change the resulting probability. If Π_j and Π'_k do commute, and only then, the joint probability of observing s_j, s'_k is independent of the measurement order for all ρ , and simplifies to

$$\mathbb{P}_\rho(\Pi_j, \Pi'_k) = \text{Tr}(\Pi'_k \Pi_j \rho).$$

2) *Multipartite systems and partial trace*: For simplicity, we present the interaction of two quantum systems; the case of $n > 2$ systems is easily obtained by iteration. If two quantum systems, with associated Hilbert spaces \mathcal{H}_1 and \mathcal{H}_2 respectively, are taken together to form a larger bipartite quantum system, the Hilbert space $\mathcal{H}_{1,2}$ associated to the composite quantum system is the tensor product of the individual quantum subsystem Hilbert spaces, $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Let $\{|\psi_k\rangle\}_{k=1}^{d_1}$ and $\{|\phi_l\rangle\}_{l=1}^{d_2}$ be orthonormal bases for \mathcal{H}_1 and \mathcal{H}_2 respectively, then an orthonormal basis for $\mathcal{H}_{1,2}$ can be written as:

$$\{|\psi_k\rangle \otimes |\phi_l\rangle\}_{k,l=1}^{d_1, d_2}, \quad (37)$$

from which we get that $\dim(\mathcal{H}_{1,2}) = \dim(\mathcal{H}_1) \dim(\mathcal{H}_2) = d_1 d_2$. We use the short notation $|\psi, \phi\rangle := |\psi\rangle \otimes |\phi\rangle$ for any $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$. The composite Hilbert space is

naturally endowed with the inner-product $\langle u_1, u_2 | v_1, v_2 \rangle := \langle u_1 | v_1 \rangle \langle u_2 | v_2 \rangle$. A representation and basis for operators in $\mathfrak{B}(\mathcal{H}_{1,2})$ is derived from its vector counterpart in the standard way. In particular, given two operators $X_1 \in \mathfrak{B}(\mathcal{H}_1)$ and $X_2 \in \mathfrak{B}(\mathcal{H}_2)$, one can define $X_1 \otimes X_2 \in \mathfrak{B}(\mathcal{H}_{1,2})$ as the linear operator such that $\forall |u_1\rangle \in \mathcal{H}_1, |u_2\rangle \in \mathcal{H}_2$:

$$X_1 \otimes X_2(|u_1\rangle \otimes |u_2\rangle) = X_1|u_1\rangle \otimes X_2|u_2\rangle \quad (38)$$

If two operators are in the form $X_1 \otimes \mathcal{I}_2$ and $\mathcal{I}_1 \otimes X_2$, i.e. they act non-trivially only on different parts of the multipartite system, then they commute for any X_1 and X_2 . It is worth noting that in matrix representation, the tensor product corresponds to the Kronecker product.

The partial trace over \mathcal{H}_1 is a linear map:

$$\text{Tr}_{\mathcal{H}_1} : \mathfrak{B}(\mathcal{H}_1 \otimes \mathcal{H}_2) \longrightarrow \mathfrak{B}(\mathcal{H}_2), \quad (39)$$

such that, for any $X_{1,2} \in \mathfrak{B}(\mathcal{H}_{1,2})$ and any $X_2 \in \mathfrak{B}(\mathcal{H}_2)$, it holds that:

$$\text{Tr}[\text{Tr}_{\mathcal{H}_1}[X_{1,2}]X_2] = \text{Tr}[X_{1,2}(\mathcal{I}_1 \otimes X_2)]. \quad (40)$$

If now $\{|\psi_k\rangle\}_{k=1}^{d_1}$ and $\{|\phi_l\rangle\}_{l=1}^{d_2}$ are orthonormal bases for \mathcal{H}_1 and \mathcal{H}_2 respectively, the partial trace over \mathcal{H}_1 can be written as:

$$\text{Tr}_{\mathcal{H}_1}[X_{1,2}] = \sum_{k,l,i} \langle \psi_k \otimes \phi_l | X_{1,2} | \psi_k \otimes \phi_l \rangle |\phi_l\rangle \langle \phi_l|. \quad (41)$$

The partial trace over \mathcal{H}_2 writes in a similar fashion.

The tensor product structure together with the superposition principle enrich quantum theory with the phenomenon of *entanglement*. Namely, if some vectors in $|\xi\rangle \in \mathcal{H}_{1,2}$ – like the above-defined basis vectors – can be *factorized* as

$$|\xi\rangle = |\psi\rangle \otimes |\phi\rangle \quad (42)$$

for some $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$, there exist many vectors in $\mathcal{H}_{1,2}$ which cannot be written like (42); these are called *entangled*.

In the density operator formalism, a state $\rho \in \mathfrak{D}(\mathcal{H}_{1,2})$ is called entangled if it cannot be written as a convex combination of factorized operators, i.e.:

$$\rho \neq \sum_i p_i \rho_i^1 \otimes \rho_i^2 \quad \text{with} \quad \rho_i^1 \in \mathfrak{D}(\mathcal{H}_1) \quad \text{and} \quad \rho_i^2 \in \mathfrak{D}(\mathcal{H}_2). \quad (43)$$

Intuitively, this means that an entangled state contains some specifically quantum correlation so that it cannot be separated into subsystem states (conditioned by classical probability correlations). The only individual characterization of a subsystem that we can give is its “expected” density operator if information about all other subsystems is ignored. This reduced density operator e.g. for subsystem 1 is obtained by taking the partial trace over \mathcal{H}_2 of the overall state ρ :

$$\bar{\rho}_1 = \text{Tr}_{\mathcal{H}_2}[\rho].$$

B. Distinguishing SSC from RSC by measurements

Accumulating statistics about measurement outcomes at each subsystem separately, allows in principle to detect a pure state for which SSC and RSC are equivalent (see Proposition 3). Indeed, the knowledge of all local measurement statistics is equivalent to knowing the reduced state.

Proposition 9: Except for the case of Proposition 3, SSC can only be distinguished from RSC by inspecting correlations between measurement outcomes at different subsystems.

Proof: The statement builds on the standard fact that the statistics of a local observable $\sigma_1 \otimes \sigma_2 \otimes \dots \otimes \sigma_m$ only depend on reduced states $\bar{\rho}_1, \bar{\rho}_2, \dots, \bar{\rho}_m$. So repeated local measurements can, at their best, fully characterize the $\bar{\rho}_k$. Checking RSC, i.e. that these $\bar{\rho}_k$ are all equal, is thus straightforward. On the other hand, reduced states $\bar{\rho}_k$ are the best that can be extracted by local measurements in trying to distinguish RSC from SSC states. If $\bar{\rho}_1 = \bar{\rho}_2 = \dots =: \bar{\rho}$ have rank one, we have the special case that is always SSC. If instead $\bar{\rho}$ has rank at least 2, we can write it as $\bar{\rho} = p_1 R_1 + p_2 R_2$ where $R_1, R_2 \in \mathfrak{B}(\mathcal{H})$, p_1, p_2 are positive scalars, R_2 is positive semidefinite, and R_1 is a projector on a 2-dimensional subspace \mathcal{V}_2 . Consider $R_1 = |e_1\rangle\langle e_1| + |e_2\rangle\langle e_2| = |f_1\rangle\langle f_1| + |f_2\rangle\langle f_2|$, where $|e_1\rangle, |e_2\rangle$ and $|f_1\rangle, |f_2\rangle$ are two orthonormal bases for \mathcal{V}_2 with $\langle e_1|f_1\rangle \notin \{0, 1\}$. Now the reconstructed $\bar{\rho}$ could equally well reflect the state

$$\rho = \bar{\rho}^{\otimes m},$$

which is SSC, or e.g. a state of the form:

$$\rho = p_2 R_2^{\otimes m} + p_1 (|e_1\rangle\langle f_1| + |e_2\rangle\langle f_2\rangle)(\langle e_1|f_1\rangle + \langle e_2|f_2\rangle)^\dagger \otimes R_1^{\otimes(m-2)},$$

where the first two subsystems are entangled. This state is not SSC, even for $m = 2$. Thus the local knowledge of $\bar{\rho}$ does not allow to distinguish if the state is SSC or not. \square

C. Proof of Proposition 1

The definition of σ SMC involves $\text{Tr}(\Pi_j^{(k)} \Pi_j^{(\ell)} \rho)$, which takes the partial trace over the state of all subsystems except the pair $\{k, \ell\}$. So we can effectively discard all but two subsystems, and show without loss of generality that it is impossible to make σ SMC hold for all σ on two subsystems $k = 1, \ell = 2$. In Proposition 4, we say that σ SMC for a particular σ requires $\Pi_{\text{sym}} \rho = \rho$ with $\Pi_{\text{sym}} = \sum_j \Pi_j^{\otimes m}$, and $\{\Pi_j\}$ the spectral projectors associated to σ . So if σ SMC has to hold for both σ and σ' , we must have in particular

$$\Pi_{\text{sym}} \Pi'_{\text{sym}} \Pi_{\text{sym}} \rho = \rho,$$

where Π'_{sym} is associated to σ' . Since $H := \Pi_{\text{sym}} \Pi'_{\text{sym}} \Pi_{\text{sym}}$ and ρ both are self-adjoint positive semidefinite, the only way to have $H\rho = \rho \neq 0$ is if H has at least one eigenvalue ≥ 1 . Now take in particular $\sigma = \sum_k k |x_k\rangle\langle x_k|$ and $\sigma' = \sum_k k |p_k\rangle\langle p_k|$, with $p_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} e^{jk2\pi i/n} |x_j\rangle$ (thus the $|p_k\rangle$ -basis is related to the $|x_k\rangle$ -basis by Fourier transform). A few computations show that H then has all eigenvalues < 1 , except for $n = 2$ that is the case of two qbits. For the latter particular case, one can prove the property by showing e.g. that there is no state which would satisfy σ SMC for all $\sigma \in \{\sigma_x, \sigma_y, \sigma_z\}$. \square

REFERENCES

- [1] D. Gorinevsky, S. Boyd, and G. Stein, "Design of low-bandwidth spatially distributed feedback," *IEEE Trans. Aut. Cont.*, vol. 53, no. 1, pp. 257–272, 2008.
- [2] B. Bamieh, F. Paganini, and M. Dahleh, "Distributed control of spatially invariant systems," *IEEE Trans. Aut. Cont.*, vol. 47, no. 7, pp. 1091–1107, 2002.
- [3] R. D'Andrea and G. Dullerud, "Distributed control design for spatially interconnected systems," *IEEE Trans. Aut. Cont.*, vol. 48, no. 9, pp. 1478–1495, 2003.
- [4] F. Bullo, J. Cortés, and S. Martínez, *Distributed control of robotic networks*. Princeton University Press, 2009.
- [5] P. Baroah and J. Hespanha, "Estimation on graphs from relative measurements: distributed algorithms and fundamental limits," *IEEE Control Systems Magazine*, vol. 27, no. 4, pp. 57–74, 2007.
- [6] V. Borkar and P. Varaiya, "Asymptotic agreement in distributed estimation," *IEEE Trans. Automatic Control*, vol. 27, no. 3, pp. 650–655, 1982.
- [7] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends in Machine Learning*, vol. 3, no. 1, pp. 1–122, 2011.
- [8] N. Leonard, D. Paley, F. Lekien, R. Sepulchre, D. Fratantoni, and R. Davis, "Collective motion, sensor networks, and ocean sampling," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 48–74, 2007.
- [9] A. Chiuso, F. Fagnani, L. Schenato, and S. Zampieri, "Gossip algorithms for simultaneous distributed estimation and classification in sensor networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 4, pp. 691–706, 2011.
- [10] J. Tsitsiklis and M. A. (advisor), "Problems in decentralized decision making and computation," *PhD Thesis, MIT*, 1984.
- [11] A. Jadbabaie, J. Lin, and A. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Trans. Automatic Control*, vol. 48, no. 6, pp. 988–1001, 2003.
- [12] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, 2007.
- [13] L. Moreau, "Stability of multi-agent systems with time-dependent communication links," *IEEE Trans. Automatic Control*, vol. 50, no. 2, pp. 169–182, 2005.
- [14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Information*. Cambridge University Press, Cambridge, 2002.
- [15] M. N. V. A. Yu. Kitaev, A. H. Shen, *Classical and Quantum Computation*. American Mathematical Society, 2002.
- [16] F. Verstraete, M. M. Wolf, and J. I. Cirac, "Quantum computation and quantum-state engineering driven by dissipation," *Nature Physics*, vol. 5, pp. 633 – 636, 2009.
- [17] J. Kempe, "Quantum random walks: An introductory overview," *Contemporary Physics*, vol. 44, no. 4, pp. 307–327, 2003.
- [18] M. Szegedy, "Quantum speed-up of Markov chain based algorithms," *Proc. 45th Annual IEEE Symp. Foundations of Computer Science*, pp. 32–41, 2004.
- [19] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, "Information preserving structures: A general framework for quantum zero-error information," *preprint*, vol. arxiv, p. 1006.1358v1, 2010.
- [20] F. Ticozzi and L. Viola, "Quantum information encoding, protection and correction via trace-norm isometries," *Phys. Rev. A*, vol. 81, no. 3, p. 032313, 2010.
- [21] —, "Quantum Markovian subsystems: Invariance, attractivity and control," *IEEE Trans. Aut. Contr.*, vol. 53, no. 9, pp. 2048–2063, 2008.
- [22] C. Ahn, H. M. Wiseman, and G. J. Milburn, "Quantum error correction for continuously detected errors," *Phys. Rev. A*, vol. 67, no. 5, pp. 052310:1–11, 2003.
- [23] F. Ticozzi and L. Viola, "Single-bit feedback and quantum dynamical decoupling," *Phys. Rev. A*, vol. 74, no. 5, pp. 052328:1–11, 2006.
- [24] B. Kraus, S. Diehl, A. Micheli, A. Kantian, H. P. Büchler, and P. Zoller, "Preparation of entangled states by dissipative quantum markov processes," *Phys. Rev. A*, vol. 78, no. 4, p. 042307, 2008.
- [25] F. Ticozzi and L. Viola, "Stabilizing entangled states with quasi-local quantum dynamical semigroups," *Phil. Trans. R. Soc. A*, vol. 370, no. 1979, pp. 5259–5269, 2012.
- [26] M. Kastoryano, M. Wolf, and J. Eisert, "Precisely timing dissipative quantum information processing," *arXiv:1205.0985*, 2012.
- [27] C. Altafini and F. Ticozzi, "Modeling and control of quantum systems: An introduction," *IEEE Trans. Aut. Cont.*, vol. 57, no. 8, pp. 1898–1917, 2012.

- [28] D. D'Alessandro, *Introduction to Quantum Control and Dynamics*, ser. Applied Mathematics & Nonlinear Science. Chapman & Hall/CRC, 2007.
- [29] M. James and J. Gough, "Quantum dissipative systems and feedback control design by interconnection," *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1806–1821, 2010.
- [30] J. Gough and M. R. James, "The series product and its application to quantum feedforward and feedback networks," *IEEE Trans. Aut. Contr.*, vol. 54, no. 11, pp. 2530–2544, 2009.
- [31] S. Bolognani and F. Ticozzi, "Engineering stable discrete-time quantum dynamics via a canonical QR decomposition," *IEEE Trans. Aut. Contr.*, vol. 55, no. 12, pp. 2721–2734, 2010.
- [32] R. F. Werner, "Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model," *Phys. Rev. A*, vol. 40, pp. 4277–4281, 1989.
- [33] T. Eggeling and R. F. Werner, "Separability properties of tripartite states with $u \otimes u \otimes u$ symmetry," *Phys. Rev. A*, vol. 63, p. 042111, 2001.
- [34] R. Sepulchre, A. Sarlette, and P. Rouchon, "Consensus in non-commutative spaces," *Proc. 49th IEEE Conf. Decision & Control*, pp. 6596–6601, 2010.
- [35] M. M. Wilde, *From classical to quantum Shannon theory*. McGill University: in preparation, 2011.
- [36] J. J. Sakurai, *Modern Quantum Mechanics*. Addison-Wesley, New York, 1994.
- [37] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory*, ser. Lecture notes in Physics. Springer-Verlag, Berlin, 1983.
- [38] C. B. Mendl and M. M. Wolf, "Unital quantum channels - convex structure and revivals of birkhoff's theorem," *Commun. Math. Phys.*, vol. 289, pp. 1057–1096, 2009.
- [39] F. Albertini and F. Ticozzi, "Discrete-time controllability for feedback quantum dynamics," *Automatica*, vol. 47, no. 11, pp. 2451–2456, 2011.
- [40] S. Lloyd and L. Viola, "Engineering quantum dynamics," *Phys. Rev. A*, vol. 65, pp. 010101:1–4, 2001.
- [41] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *IEEE Trans. Information Theory (Special issue)*, vol. 52, no. 6, pp. 2508–2530, 2006.
- [42] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications*. Springer-Verlag, Berlin, 1987.