# Privacy Preserving Average Consensus

Yilin Mo, *Member, IEEE*, Richard M. Murray, *Fellow, IEEE*

**Abstract**

Average consensus is a widely used algorithm for distributed computing and control, where all the agents in the network constantly communicate and update their states in order to achieve an agreement. This approach could result in an undesirable disclosure of information on the initial state of an agent to the other agents. In this paper, we propose a privacy preserving average consensus algorithm to guarantee the privacy of the initial state and asymptotic consensus on the exact average of the initial values, by adding and subtracting random noises to the consensus process. We characterize the mean square convergence rate of our consensus algorithm and derive the covariance matrix of the maximum likelihood estimate on the initial state. Moreover, we prove that our proposed algorithm is optimal in the sense that it does not disclose any information more than necessary to achieve the average consensus. A numerical example is provided to illustrate the effectiveness of the proposed design.

**Index Terms**

Privacy, Multi-agent systems, Networked control systems, Estimation

## I. Introduction

Consensus has been an active research area over the past decades. Early researches use consensus to model and analyze phenomena such as agreement of opinions by a group of individuals [1] and decision making by decentralized processors [2]. Applications of distributed averaging algorithms include dynamic load balancing [3], coordination of groups of mobile autonomous agents [4] and cooperative control of vehicle formations [5]. A survey of theory

Yilin Mo is with the School of Electrical and Electronic Engineering, Nanyang Technological University. Email: ylmo@ntu.edu.sg

Richard M. Murray are with the Control and Dynamical Systems Department of the California Institute of Technology. Email: murray@cds.caltech.edu

This work is supported in part by IBM and UTC through iCyPhy consortium.

and applications of consensus problems in networked systems can be found in [6]. Consensus problems in the context of distributed signal processing applications, such as distributed parameter estimation, source localization and distributed compression have been reviewed in [7].

One commonly adopted consensus scheme is the deterministic average consensus algorithm, where each agent communicates with a fixed set of neighbors and follows a time-invariant update algorithm to reach the average of their initial values. In this approach, if one agent knows the update rules of all the other agents, then under some observability conditions, it can infer the state of all the other agent. This may turn out to be desirable for some applications, such as malicious intrusion detection and identification [8] and finite-step consensus [9], [10]. However, it also implies that the exact initial value of one agent may be computable by the other agents, which results in a disclosure of information. For privacy concerns, the participating agents may not want to release more information on its initial value than strictly necessary to reach the average consensus. For example, in social networks, a group of individuals can employ consensus algorithm to compute the common opinion on a subject [1]. However, they may not want to reveal their exact personal opinion on the subject. Another example is the multi-agent rendezvous problem [11], where a group of agents want to eventually rendezvous at a certain location. In this application, the participating agents may want to keep their initial location secret to the others.

In the database literature, the concept of differential privacy [12] has been extensively studied in the recent years. A widely adopted differentially private mechanism is to return a randomized answer to any database query to guarantee that the data from any individual participant of the database will only marginally change the distribution of the randomized answer [13]. Recently, the concept of differential privacy has been applied in dynamical systems. In [14], the authors consider the design of differentially private filters for dynamical system by adding white Gaussian perturbations to the system. In the context of consensus problem, Huang et al. [15] propose a differentially private consensus algorithm, where an independent and exponentially decaying Laplacian noise process is added to the consensus computation. However, their consensus algorithm does not converge to the *exact* average of the initial value, but to a randomized value. As a result, it cannot be applied to the case where the exact average consensus is required. Manitara and Hadjicostis [16] propose a privacy preserving average consensus scheme by adding correlated noise and discuss whether the initial state of one agent can be perfectly inferred by the other "malicious" agents. However, they do not provide a quantitative result on how good the initial state can be estimated. Moreover, they can only provide a sufficient condition under which the privacy of the benign agents are preserved. Xue et al. [17] consider the privacy problem in autonomous vehicle networks with a canonical Double-Integrator-Network model when the system is either noise-free or subject to white Gaussian observation noise.

In this paper, we propose a privacy preserving average consensus algorithm, which computes the *exact* average of the initial values and ensures that the initial value of an agent cannot be perfectly inferred by the other participating agents. The requirement of the exact average consensus proposes new challenges, as one need to design a correlated noise process to ensure that the noise does not affect the consensus result. Hence, the techniques developed in [14], [15] cannot be directly applied to the average consensus case.

A preliminary version of these results is available in [18]. In this paper the analysis is extended in the following directions:

- We derive the *exact* asymptotic estimation performance $P$.
- We consider a general consensus scheme and prove that our privacy preserving consensus algorithm achieves minimum privacy breach.

The rest of the paper is organized as follows: in Section II, we provide a brief introduction of the average consensus algorithm. A privacy preserving average consensus algorithm is proposed in Section III and its properties are proved in Section IV. In Section V, we consider a more general consensus framework and prove that our algorithm discloses the minimum amount of information among all possible average consensus algorithms. An illustrative example on a simple cyclic network is presented in Section VI. Finally, Section VII concludes the paper.

**Notations:** $\mathbb{N}$ is the set of non-negative integers. $\mathbb{R}^{n\times m}$ is the set of $n$ by $m$ matrices. $\mathbb{S}^n$ is the set of $n$ by $n$ symmetric matrices. The $i$th diagonal entry of the matrix $X$ is denoted as $X_{ii}$. All the comparisons between matrices in this article are in positive semidefinite sense. $\mathbf{1}$ and $\mathbf{0}$ are all one and all zero vectors of proper dimension respectively. $\mathrm{range}(X), \mathrm{null}(X)$ represent the column space and the null space of the matrix $X$. $\|v\|$ indicates the 2-norm of the vector $v$, while $\|X\|$ is the largest singular value of the matrix $X$.

## II. Preliminaries

In this section we briefly introduce the average consensus algorithm, the notation of which will be used later in the paper.

We model a network composed of $n$ agents as a graph $G = \{V, E\}$. $V = \{1, 2, \ldots, n\}$ is the set of vertices representing the agents. $E \subseteq V \times V$ is the set of edges. $(i, j) \in E$ if and only if agent $i$ and $j$ can communicate directly with each other. In this paper we always assume that $G$ is *undirected and connected*. The neighborhood of agent $i$ is defined as

$$\mathcal{N}(i) \triangleq \{j \in V : (i, j) \in E, \, j \neq i\}.$$

Suppose that each agent has an initial scalar state $x_i(0)$. At each iteration, agent $i$ will communicate with its neighbors and update its state according to the following equation:

$$x_i(k+1) = a_{ii}x_i(k) + \sum_{j \in \mathcal{N}(i)} a_{ij}x_j(k). \tag{1}$$

Define $x(k) \triangleq [x_1(k), \ldots, x_n(k)]' \in \mathbb{R}^n$ and $A \triangleq [a_{ij}] \in \mathbb{R}^{n \times n}$. The update equation (1) can be written in matrix form as

$$x(k+1) = Ax(k). \tag{2}$$

In the rest of the paper, $A$ is assumed to be *symmetric*. Define the essential neighborhood $\mathcal{N}_e(i)$ of an agent $i$ to be the set of neighboring agents whose information is used to compute (1), i.e.,

$$\mathcal{N}_e(i) \triangleq \{j \in \mathcal{N}(i) : a_{ij} \neq 0\}. \tag{3}$$

Furthermore, define the average vector and the error vector to be

$$\bar{x} \triangleq \frac{\mathbf{1}'x(0)}{n}\mathbf{1}, \; z(k) \triangleq x(k) - \bar{x}.$$

The goal of the average consensus is to guarantee that $z(k) \to 0$ as $k \to \infty$ through the update equation (2). Let us arrange the eigenvalues of $A$ in the decreasing order as $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n$. It is well known that the following conditions are necessary and sufficient in order to achieve average consensus from any initial condition $x(0)$:

(A1) $\lambda_1 = 1$ and $|\lambda_i| < 1$ for all $i = 2, \ldots, n$.

(A2) $A\mathbf{1} = \mathbf{1}$, i.e., $\mathbf{1}$ is an eigenvector of $A$.

For the rest of the paper, we assume that $A$ satisfies Assumption (A1) and (A2).

## III. Problem Formulation

One issue for the average consensus algorithm is that an agent in the network could potentially infer the other agents' exact initial condition $x_i(0)$s, which may not be desirable when privacy is of concern.

To avoid privacy breaches while enforcing that $x(k)$ converges to $\bar{x}$, we propose the following privacy preserving average consensus algorithm:

**Algorithm 1.** 1) *At time $k$, each agent generates a standard normal distributed random variable $v_i(k)$ with mean $0$ and variance 1. We assume that all the random variables $\{v_i(k)\}_{i=1,\ldots,n,\,k=0,1,\ldots}$ are jointly independent.*

2) *Each agent then adds a random noise $w_i(k)$ to its state $x_i(k)$, where*

$$w_i(k) = \begin{cases} v_i(0) & \text{, if } k = 0 \\ \varphi^k v_i(k) - \varphi^{k-1} v_i(k-1) & \text{, otherwise} \end{cases}, \tag{4}$$

*where $0 < \varphi < 1$ is a constant for all agents. Define the new state to be $x_i^+(k)$, i.e.,*

$$x_i^+(k) = x_i(k) + w_i(k). \tag{5}$$

3) *Each agent then communicates with its neighbors and update its state to the average value, i.e.,*

$$x_i(k+1) = a_{ii} x_i^+(k) + \sum_{j \in \mathcal{N}(i)} a_{ij} x_j^+(k). \tag{6}$$

4) *Advance the time to $k+1$ and go to step 1).*

Define

$$w(k) \triangleq [w_1(k), \ldots, w_n(k)]' \in \mathbb{R}^n, \tag{7}$$

$$v(k) \triangleq [v_1(k), \ldots, v_n(k)]' \in \mathbb{R}^n, \tag{8}$$

$$x^+(k) \triangleq [x_1^+(k), \ldots, x_n^+(k)]' \in \mathbb{R}^n. \tag{9}$$

We can write (5) and (6) in matrix form as

$$x(k+1) = Ax^+(k) = A(x(k) + w(k)). \tag{10}$$

**Remark 1.** *Our noise model is motivated by the following requirements:*

1) *The consensus algorithm needs to converge.*
2) *All nodes reach consensus on the exact average.*

*As a result, the noise needs to be decaying to ensure convergence and the asymptotic sum of the noise needs to be* $0$ *to avoid affecting the consensus results. The noise is chosen to be Gaussian so that the maximum likelihood estimator is efficient and unbiased. Furthermore, the maximum likelihood estimator can be written in an analytical form for Gaussian noise. On the other hand, for other noise models, such as Laplacian noise, a closed form maximum likelihood estimator may not exist. Nevertheless, in Section V, we will consider general noise model and prove that our noise design* (4) *has minimum privacy breach.*

*Finally, We choose the variance of* $v_i(k)$ *to be* $1$ *to simplify the notations. With proper scaling, all the results in this article hold when Var*$(v_i(k)) = \sigma^2$.

**Remark 2.** *It is worth noticing that the proposed algorithm does not require additional communication structure, which may be desirable if the communication resources are limited. On the other hand, the problem may become easier if secret communication channels can be established between agents.*

*Furthermore, it is worth mentioning that privacy can be easily achieved if only the consensus on* **some** *value is needed, since one has more freedom to design the noise process* $\{w(k)\}$. *For instant, one can choose* $w(k)$ *to be mutually independent with an exponentially decaying covariance matrix [15]. On the other hand, to achieve the exact average consensus, one has to ensure that the added noise process* $\{w(k)\}$ *does not affect the consensus result, which implies that* $\{w(k)\}$ *must be correlated.*

Without loss of generality, we only consider the case where agent $n$ wants to infer the other agents' initial conditions. Denote the neighborhood of agent $n$ as

$$\mathcal{N}(n) = \{j_1, \ldots, j_m\}.$$

Define

$$C \triangleq \begin{bmatrix} e_{j_1} & \ldots & e_{j_m} & e_n \end{bmatrix}' \in \mathbb{R}^{(m+1)\times n}, \tag{11}$$

where $e_i$ denotes the $i$th canonical basis vector in $\mathbb{R}^n$ with a $1$ in the $i$th entry and zeros elsewhere. The information set of agent $n$ at time $k$ can be defined as

$$\mathcal{I}(k) \triangleq \{x_n(0), y(0), \ldots, y(k)\}, \tag{12}$$

where

$$y(k) \triangleq Cx^{+}(k) = C(x(k) + w(k)). \tag{13}$$

Notice that $x_n(k+1), k = 0, 1, \ldots$ is not included in the information set since it can be directly computed from $y(k)$ using (6). We assume that agent $n$ knows the $A$ and $C$ matrices and all the variables in $\mathcal{I}(k)$ at time $k$.

**Remark 3.** *Without the additional noise, i.e.,* $w(k) = 0$*, the consensus algorithm is deterministic and agent* $n$ *can perfectly infer* $\zeta' x(0)$*, given that* $\zeta \in \mathbb{R}^n$ *lies in the observable space of* $(A, C)$*, which illustrates the necessity of the added noise.*

Denote the maximum likelihood estimate of $x(0)$ given $\mathcal{I}(k)$ as $\hat{x}(0|k)$, the variance of which is defined as $P(k)$. Since $\mathcal{I}(k) \subset \mathcal{I}(k+1)$, we have the following proposition:

**Proposition 1.** $P(k)$ *is monotonically non-increasing, i.e.,* $P(k_2) \le P(k_1)$ *if* $k_1 \le k_2$*.*

Hence, the following limit is well-defined:

$$P \triangleq \lim_{k \to \infty} P(k). \tag{14}$$

Since the noises $v_i(k)$ are independently Gaussian distributed, the maximum likelihood estimator is the minimum variance unbiased estimator. As a result, the matrix $P$ determines the fundamental limit on how accurate $x(0)$ can be estimated by agent $n$. If there exists an vector $\zeta \in \mathbb{R}^n$, such that

$$\zeta' P \zeta = 0,$$

then if agent $n$ wants to estimate $\zeta' x(0)$, it could use $\zeta' \hat{x}(0|k)$ as the maximum likelihood estimate of $\zeta' x(0)$ at time $k$. Notice that the variance of such an estimate at time $k$ is given by $\zeta' P(k) \zeta$, which asymptotically converges to 0. Hence, if $\zeta' P \zeta = 0$, then agent $n$ can asymptotically infer a linear combination of the initial state $\zeta' x(0)$ without any error. On the other hand, if

$$\zeta' P \zeta > 0,$$

then agent $n$ cannot perfectly estimate $\zeta' x(0)$ even if it has collected an infinite number of measurements $\mathcal{I}(\infty)$. This observation leads to the following definition:

**Definition 1.** *A vector $\zeta \in \mathbb{R}^n$ is called a disclosed vector if and only if $\zeta' P \zeta = 0$. Further define the disclosed subspace $\mathbb{D}$ as the null space of $P$.*

By definition, if the $i$th canonical basis vector $e_i \in \mathbb{D}$ is in the disclosed subspace, then agent $n$ can asymptotically infer $e_i' x(0) = x_i(0)$, which implies that the privacy of the agent $i$ is breached. On the other hand, if $e_i \notin \mathbb{D}$, then agent $n$ cannot perfectly infer $x_i(0)$, which leads to the following definition:

**Definition 2.** *The initial condition $x_i(0)$ of agent $i$ is kept private (from agent $n$) if and only if $e_i \notin \mathbb{D}$.*

In the next section, we first prove that we can achieve average consensus using the proposed scheme. We then provide an exact characterization on the matrix $P$ and the disclosed space $\mathbb{D}$.

## IV. Main Results

In this section, we first characterize the convergence rate of the privacy preserving average consensus algorithm. We then compute $P$ and the disclosed space $\mathbb{D}$.

### A. Convergence Rate

We consider the impact of the added noise $w(k)$ on the performance of the consensus algorithm. Let us define the mean square convergence rate $\rho$ of our consensus algorithm as

$$\rho \triangleq \lim_{k\to\infty} \left( \sup_{z(0)\neq 0} \frac{\mathbb{E} z(k)' z(k)}{z(0)' z(0)} \right)^{1/k}, \tag{15}$$

whenever the limit on the RHS exists. The expectation is taken over the noise process. The following theorem establish the convergence properties of $x(k)$:

**Theorem 1.** *For any initial condition $x(0)$, $x(k)$ converges to $\bar{x}$ in the mean square sense. Furthermore, the mean square convergence rate $\rho$ equals*

$$\rho = \max(\varphi^2, |\lambda_2|^2, |\lambda_n|^2). \tag{16}$$

The following lemma is needed to prove Theorem 1:

**Lemma 1.** *Define matrix $\mathcal{A}$ to be*

$$\mathcal{A} \triangleq A - \mathbf{1}\mathbf{1}'/n.$$

*The following equalities hold for all $k \geq 0$*

$$A^k(A-I) = \mathcal{A}^k(A-I), \tag{17}$$

$$A^k - \mathbf{1}\mathbf{1}'/n = \mathcal{A}^k(I - \mathbf{1}\mathbf{1}'/n). \tag{18}$$

*Proof.* By Assumption (A1) and (A2), the following equalities hold

$$\frac{\mathbf{1}\mathbf{1}'}{n}A = \frac{\mathbf{1}\mathbf{1}'}{n} = A\frac{\mathbf{1}\mathbf{1}'}{n}.$$

As a result, $\mathcal{A}^k = A^k - \mathbf{1}\mathbf{1}'/n$. (17) and (18) can be proved by replacing $\mathcal{A}^k$ by $A^k - \mathbf{1}\mathbf{1}'/n$ on the RHS respectively. $\square$

*Proof of Theorem 1.* Since the RHS of (16) is strictly less than 1, we only need to prove (16), since it implies the mean square convergence. By (10),

$$\begin{aligned} x(k) &= A^k x(0) + \sum_{t=0}^{k-1} A^{k-t} w(t) \\ &= A^k x(0) + A\varphi^{k-1} v(k-1) + \sum_{t=0}^{k-2} \varphi^t A^{k-t-1}(A-I)v(t). \end{aligned}$$

Since $\bar{x} = (\mathbf{1}\mathbf{1}'/n)x(0)$, by Lemma 1, we have

$$z(k) = \mathcal{A}^k z(0) + A\varphi^{k-1} v(k-1) + \sum_{t=0}^{k-2} \varphi^t \mathcal{A}^{k-t-1}(A-I)v(t).$$

Since $\{v(k)\}$ are i.i.d. Gaussian vectors with zero mean and covariance $I$, the mean square error can be written as

$$\begin{aligned} \mathbb{E}z(k)'z(k) &= z(0)'\mathcal{A}^{2k}z(0) + \operatorname{tr}(A^2)\varphi^{2k-2} \\ &\quad + \sum_{t=0}^{k-2} \varphi^{2t} \operatorname{tr}\left[\mathcal{A}^{2k-2t-2}(A-I)^2\right]. \end{aligned} \tag{19}$$

Since all the terms on the RHS of (19) are non-negative,

$$\mathbb{E}z(k)'z(k) \geq z(0)'\mathcal{A}^{2k}z(0), \mathbb{E}z(k)'z(k) \geq \operatorname{tr}(A^2)\varphi^{2k-2},$$

which implies that

$$\rho \geq \max(\varphi^2, |\lambda_2|^2, |\lambda_n|^2).$$

On the other hand, since the eigenvalues of $A$ are $\lambda_1, \dots, \lambda_n$, we have

$$\begin{aligned}
&\sum_{t=0}^{k-2} \varphi^{2t} \operatorname{tr}\left[\mathcal{A}^{2k-2t-2}(A-I)^2)\right] \\
&= \sum_{i=2}^{n} \sum_{t=0}^{k-2} \left(\varphi^{2t}\lambda_i^{2k-2t-2}\right)(\lambda_i - 1)^2 \\
&\le (n-1)(k-1)\left[\max(\varphi, |\lambda_2|, |\lambda_n|)\right]^{2k-2}(\lambda_n - 1)^2
\end{aligned}$$

The last inequality is true due to the fact that for all $t$,

$$\left(\varphi^{2t}\lambda_i^{2k-2t-2}\right)(\lambda_i - 1)^2 \le \left[\max(\varphi, |\lambda_2|, |\lambda_n|)\right]^{2k-2}(\lambda_n - 1)^2.$$

Combining with (19), we can prove that

$$\rho \le \max(\varphi^2, |\lambda_2|^2, |\lambda_n|^2).$$

which finishes the proof. □

### *B. Estimation Performance*

In this subsection, we provide upper and lower bounds on $P$. Notice that our goal is not to design an estimator for agent $n$, but rather to prove a fundamental limit on the performance for all possible unbiased estimators, which guarantees the privacy of $x(0)$. We first reduce the state space by removing $x_n(k)$, since it is already known to agent $n$. To this end, let us define $\tilde{A} \in \mathbb{R}^{(n-1)\times(n-1)}$ as a principal minor of $A$ by removing the last row and column. As a result, the matrix $A$ can be written as

$$A = \begin{bmatrix} \tilde{A} & \eta \\ \eta' & a_{nn} \end{bmatrix}, \tag{20}$$

where $\eta \in \mathbb{R}^{n-1}$. The following lemma characterize the stability of $\tilde{A}$, the proof of which is reported in the appendix:

**Lemma 2.** *$\tilde{A}$ is strictly stable, i.e., $\|\tilde{A}\| < 1$. Furthermore, for any $i$, $\tilde{A}_{ii} < 1$.*

Let us further define the reduced noise vector as

$$\tilde{v}(k) \triangleq \begin{bmatrix} v_1(k) & \dots & v_{n-1}(k) \end{bmatrix}' \in \mathbb{R}^{n-1}, \tag{21}$$

$$\tilde{w}(k) \triangleq \begin{bmatrix} w_1(k) & \dots & w_{n-1}(k) \end{bmatrix}' \in \mathbb{R}^{n-1}, \tag{22}$$

We define the reduced state vector $\tilde{x}(k) \in \mathbb{R}^{n-1}$, which satisfies the following update equation:

$$\tilde{x}(k+1) = \tilde{A}(\tilde{x}(k) + \tilde{w}(k)), \tag{23}$$

with initial condition

$$\tilde{x}(0) \triangleq \begin{bmatrix} x_1(0) & \dots & x_{n-1}(0) \end{bmatrix}' \tag{24}$$

**Remark 4.** *Roughly speaking, $\tilde{x}(k)$ represents the state of the agent $1, ..., n-1$ after removing the influence from agent $n$. It is worth noticing that in general, $\tilde{x}(k) \neq \begin{bmatrix} x_1(k) & \dots & x_{n-1}(k) \end{bmatrix}'$.*

Finally, let us define the reduced $\tilde{C}$ matrix as

$$\tilde{C} \triangleq \begin{bmatrix} \tilde{e}_{j_1} & \dots & \tilde{e}_{j_m} \end{bmatrix}' \in \mathbb{R}^{m \times (n-1)}, \tag{25}$$

where $\tilde{e}_i$ denotes the $i$th canonical basis vector in $\mathbb{R}^{n-1}$. The reduced measurement $\tilde{y}(k) \in \mathbb{R}^m$ is defined as

$$\tilde{y}(k) \triangleq \tilde{C}(\tilde{x}(k) + \tilde{w}(k)). \tag{26}$$

Throughout the subsection, we assume that $(\tilde{A}, \tilde{C})$ is *observable*. Otherwise, one can always perform a Kalman decomposition and consider only the observable subspace. Define the information set based on the reduced measurements

$$\tilde{\mathcal{I}}(k) \triangleq \{x_n(0), w_n(0), \dots, w_n(k), \tilde{y}(0), \dots, \tilde{y}(k)\}. \tag{27}$$

The following theorem establishes the equivalence between information set $\mathcal{I}(k)$ and $\tilde{\mathcal{I}}(k)$, the proof of which is reported in the appendix for the sake of legibility.

**Theorem 2.** *For any $k \geq 0$, there exists an invertible linear transformation from the row vector*

$$\begin{bmatrix} x_n(0) & y(0)' & \dots & y(k)' \end{bmatrix}$$

*to the row vector*

$$\begin{bmatrix} x_n(0) & w_n(0) & \dots & w_n(k) & \tilde{y}(0)' & \dots & \tilde{y}(k)' \end{bmatrix}.$$

By Theorem 2, $\tilde{\mathcal{I}}(k)$ is a sufficient statistic for estimating $x(0)$. It is easy to see that $\{\tilde{y}(0), \dots, \tilde{y}(k)\}$ is a sufficient statistics for estimating $\tilde{x}(0)$. Therefore, let us define $\tilde{P}(k)$ as the covariance of the maximum likelihood estimate of $\tilde{x}(0)$ given $\tilde{y}(0), \dots, \tilde{y}(k)$. Since $x_n(0)$ is known to agent $n$, we have the following proposition:

**Proposition 2.** *$P(k)$ satisfies the following equality:*

$$P(k) = \begin{bmatrix} \tilde{P}(k) & \mathbf{0} \\ \mathbf{0}' & 0 \end{bmatrix}.$$

**Remark 5.** *It is worth noticing that throughout the paper we assume that agent $n$ will follow the update procedure described by Algorithm 1. However, one can easily apply the results derived in this subsection to the case where the agent $n$ does not follow the normal consensus protocol, since estimation performance is derived using the reduced system, which represents the system after removing the influence of the agent $n$. This can be seen as a special case of the separation principle, where the estimation of the initial state is independent of the malicious actions (not following the protocol) from agent $n$.*

*Moreover, the results derived in this subsection can be easily extended to the case where multiple agents want to collaboratively infer the initial conditions of the other agents, by defining the corresponding reduced system.*

Before stating the main theorem, we need to define the following projection matrices:

$$\mathcal{U} \triangleq \tilde{C}'\tilde{C} \in \mathbb{R}^{(n-1)\times(n-1)},\ \mathcal{V} \triangleq I - \mathcal{U}. \tag{28}$$

Further denote the eigenvectors of the symmetric matrix $(I-\tilde{A})^{-1}\mathcal{U}(I-\tilde{A})^{-1}$ as $\psi_1, \dots, \psi_{n-1} \in \mathbb{R}^{n-1}$. Without loss of generality, we assume that $\{\psi_1, \dots, \psi_{n-1}\}$ forms an orthonormal basis of $\mathbb{R}^{n-1}$. Furthermore, by Lemma 2 and (25), we know that

$$\text{rank}\left[(I-\tilde{A})^{-1}\mathcal{U}(I-\tilde{A})^{-1}\right] = m.$$

Hence, without loss of generality we assume that the eigenvalues corresponding to the eigenvectors $\{\psi_1, \dots, \psi_m\}$ are non-zero and the eigenvalues corresponding to $\{\psi_{m+1}, \dots, \psi_{n-1}\}$ are zero. Define the orthogonal matrix

$$\mathcal{Q} \triangleq \begin{bmatrix} \mathcal{Q}_1 & \mathcal{Q}_2 \end{bmatrix} \in \mathbb{R}^{(n-1)\times(n-1)}, \tag{29}$$

where

$$\mathcal{Q}_1 \triangleq \begin{bmatrix} \psi_1 & \dots & \psi_m \end{bmatrix} \in \mathbb{R}^{(n-1)\times m}, \tag{30}$$

$$\mathcal{Q}_2 \triangleq \begin{bmatrix} \psi_{m+1} & \dots & \psi_{n-1} \end{bmatrix} \in \mathbb{R}^{(n-1)\times(n-m-1)}. \tag{31}$$

We are now ready to state the main theorem, the proof of which is reported in the appendix for the sake of legibility.

**Theorem 3.** *Suppose that* $\varphi \in (0,1)$. $\tilde{P}$ *is given by the following equality:*

$$\tilde{P} = \mathcal{Q}_2 \left[\mathcal{Q}_2'(I-\tilde{A})^{-1} Y (I-\tilde{A})^{-1}\mathcal{Q}_2\right]^{-1} \mathcal{Q}_2', \tag{32}$$

*where* $Y = \lim_{k\to\infty} Y(k)$ *is the limit of the following recursive Riccati equations:*

$$Y(0) = \tilde{A}\mathcal{U}\tilde{A}, \tag{33}$$

$$\begin{aligned} Y(k+1) &= \tilde{A}\mathcal{U}\tilde{A} \\ &+\varphi^{-2}\tilde{A}\left[Y^+(k) - Y^+(k)\left(\varphi^2 I + Y^+(k)\right)^{-1} Y^+(k)\right]\tilde{A}, \end{aligned} \tag{34}$$

*where*

$$Y^+(k) = \mathcal{V} Y(k) \mathcal{V}. \tag{35}$$

The following theorem characterizes the disclosed space:

**Theorem 4.** *The disclosed space* $\mathbb{D}$ *is given by*

$$\mathbb{D} = \left\{ \begin{bmatrix} \tilde{\zeta} \\ 0 \end{bmatrix} \in \mathbb{R}^n : \tilde{\zeta} \in \mathit{range}(\mathcal{Q}_1) \right\} \oplus \{ t e_n : t \in \mathbb{R} \}, \tag{36}$$

*where* $e_n = \begin{bmatrix} 0 & \dots & 0 & 1 \end{bmatrix}'$*, and* $\oplus$ *denotes the direct sum of subspaces.*

*Proof.* By Proposition 2, $e_n' P e_n = 0$, which implies that $e_n \in \mathbb{D}$. Now consider a vector $\begin{bmatrix} \tilde{\zeta}' & 0 \end{bmatrix}'$ that is perpendicular to $e_n$. It is a disclosed vector if and only if $\tilde{\zeta}'\tilde{P}\tilde{\zeta} = 0$, which is equivalent to $\mathcal{Q}_2'\tilde{\zeta} = 0$. As a result, $\tilde{\zeta}$ belongs to the null space of $\mathcal{Q}_2'$, which is also the column space of $\mathcal{Q}_1$. □

The following corollary provides a topological condition on the computability of $x_i(0)$ for agent $n$:

**Corollary 1.** *Let* $e_i \in \mathbb{R}^n$ *be the ith canonical basis vector.* $e_i \in \mathbb{D}$ *if and only if* $i = n$ *or* $\mathcal{N}_e(i) \bigcup \{i\} \subseteq \mathcal{N}(n) \bigcup \{n\}$.

*Proof.* Consider the case where $i \neq n$. By definition, the column space of $\mathcal{Q}_1$ is the column space of $(I - \tilde{A})^{-1}\tilde{C}'$. Therefore, $e_i \in \mathbb{D}$ is equivalent to

$$\tilde{e}_i - \tilde{A}\tilde{e}_i \in \text{range}(\tilde{C}'),$$

where $\tilde{e}_i \in \mathbb{R}^{n-1}$ is the $i$th canonical basis vector of $\mathbb{R}^{n-1}$. By (25), a vector $\tilde{v} \in \text{range}(\tilde{C}')$ if and only if $\tilde{v}_j = 0$ for all $j \notin \mathcal{N}(n)$. By Lemma 2, the $j$th entry of $\tilde{e}_i - \tilde{A}\tilde{e}_i$ is 0 if and only if $j \notin (\mathcal{N}_e(i) \bigcup \{i\}) \setminus \{n\}$. Hence, $P_{ii} = 0$ is equivalent to $\mathcal{N}_e(i) \bigcup \{i\} \subseteq \mathcal{N}(n) \bigcup \{n\}$. $\square$

By Corollary 1, as long as agent $n$ cannot listen to agent $i$ and all its essential neighbors, agent $n$ cannot estimate the initial condition $x_i(0)$ perfectly. Notice that this result is independent from the choice of $\varphi$. Hence, we can potentially use a small $\varphi$ that does not degrade the consensus performance while achieving the privacy of $x(0)$.

Moreover, to enforce the privacy of the initial condition $x_i(0)$ of node $i$ to all other node $j$, we should enforce that for any $j \neq i$, the following holds:

$$\mathcal{N}_e(i) \bigcup \{i\} \nsubseteq \mathcal{N}(j) \bigcup \{j\}. \tag{37}$$

It is worth noticing that (37) can be verified locally. In particular, to falsify (37), $j$ has to be a neighbor of $i$. In other words, the initial condition of agent $i$ can only be leaked to its neighboring agents. As a consequence, $i$ only need to enforce (37) for each neighboring agent $j$ to ensure that its initial condition cannot be estimated perfectly by any other node.

On the other hand, suppose at most $k$ nodes are trying to estimate $x(0)$ collaboratively. In that case, to ensure the privacy of node $i$, $i$ needs to ensure that the following condition holds for all combinations of $k$ nodes $j_1, \ldots, j_k \neq i$:

$$\mathcal{N}_e(i) \bigcup \{i\} \nsubseteq \mathcal{N}(j_1) \bigcup \cdots \bigcup \mathcal{N}(j_k) \bigcup \{j_1, j_2, \ldots, j_k\}. \tag{38}$$

In fact, node $i$ only needs to check those $j_i$s that are either its neighbor or two-hop neighbors since otherwise

$$\left\{\mathcal{N}_e(i) \bigcup \{i\}\right\} \bigcap \left\{\mathcal{N}(j_i) \bigcup \{j_i\}\right\} = \emptyset.$$

This implies that (38) can also be verified locally.

## V. Fundamental Limits on Privacy for Average Consensus

By Theorem 4, the disclosed space of an agent with $m$ neighbors is of dimension $m+1$. One may wonder if this privacy "breach" is caused by our specific noise process defined by (4). In this section, we consider a more general consensus scheme and prove that for any average consensus algorithm given by (10), if the noise processes satisfies an independent assumption, then the dimension of the disclosed space will be at least $m+1$. As a result, our proposed algorithm is optimal in the sense that it does not disclose any information more than necessary to achieve the average consensus.

To this end, let us consider the following general consensus algorithm:

1) At time $k$, each agent adds a zero mean random noise $w_i(k)$ to its state $x_i(k)$. Define the new state to be $x_i^+(k)$, i.e.,
$$x_i^+(k) = x_i(k) + w_i(k). \tag{39}$$
2) Each agent then communicates with its neighbors and update its state to the average value, i.e.,
$$x_i(k+1) = a_{ii}x_i^+(k) + \sum_{j\in\mathcal{N}(i)} a_{ij}x_j^+(k). \tag{40}$$

We make the following independent assumption on the noise $w_i(k)$:

(A3) $\mathbb{E}w_i(k_1)w_j(k_2) = 0$ if $i \neq j$.

**Remark 6.** *It is worth noticing that the noise $w_i(k_1)$ and $w_i(k_2)$ generated by the same agent $i$ can be correlated, as is the case in* (4)*. In practice, Assumption (A3) implies that the agents are not collaborating when generating the noise.*

In the hope of improving the legibility of the paper, we will slight abuse the notation by adopting all the symbols defined in Section III and IV.

Let us further define the sum of the noise $w_i(k)$ as
$$u_i(k) \triangleq \sum_{t=0}^{k} w_i(t). \tag{41}$$

Since the statistics of the noise $w_i(k)$ is unspecified, an efficient estimator may not exist and the matrix $P$ may not be well-defined. As a result, we generalize our definition of disclosed vector as follows:

**Definition 3.** *A vector $\zeta \in \mathbb{R}^n$ is called a disclosed vector if and only if there exists a sequence $\{\hat{\theta}(k)\}$, where $\hat{\theta}(k)$ is a function of $\mathcal{I}(k)$ and*

$$\lim_{k\to\infty} \mathbb{E}(\hat{\theta}(k) - \zeta' x(0))^2 = 0.$$

One can view $\hat{\theta}(k)$ as an estimate (not necessarily the maximum likelihood estimate) of $\zeta' x(0)$ at time $k$. For the Gaussian case discussed in Section IV, one can take $\hat{\theta}(k) = \zeta' \hat{x}(0|k)$ to prove that the definition of the disclosed vector for the general case coincides with Definition 1.

If $\zeta_1$ and $\zeta_2$ are both disclosed vectors, then any linear combination of them is also a disclosed vector. Therefore, we can also generalize the concept of disclosed subspace as follows:

**Definition 4.** *The disclosed subspace $\mathbb{D}$ (of agent $n$) is given by*

$$\mathbb{D} \triangleq \{\zeta \in \mathbb{R}^n : \zeta \text{ is a disclosed vector}\}. \tag{42}$$

The following theorem provides a necessary condition for the consensus algorithm to converges to the average.

**Theorem 5.** *Suppose Assumption (A3) holds, then $x(k)$ converges to $\bar{x}$ in the mean squared sense, i.e.,*

$$\lim_{k\to\infty} \mathbb{E} \left\| x(k) - \bar{x} \right\|^2 = 0, \tag{43}$$

*implies that*

$$\lim_{k\to\infty} \mathbb{E}\, u_i(k)^2 = 0, \ \forall i = 1, \dots, n. \tag{44}$$

*Proof.* Multiplying both the LHS and RHS of (10) by $\mathbf{1}'$, we get

$$\mathbf{1}' x(k+1) = \mathbf{1}' x(k) + \mathbf{1}' w(k).$$

Thus, $\mathbf{1}' x(k+1) = \mathbf{1}' x(0) + \sum_{i=1}^n u_i(k)$. Since $\mathbf{1}' x(0) = \mathbf{1}' \bar{x}$, (43) implies that

$$\lim_{k\to\infty} \mathbb{E} \left( \sum_{i=1}^n u_i(k) \right)^2 = 0.$$

By Assumption (A3), $\mathbb{E} u_i(k) u_j(k) = 0$. Therefore,

$$\lim_{k\to\infty} \sum_{i=1}^n \left( \mathbb{E} u_i(k)^2 \right) = \lim_{k\to\infty} \mathbb{E} \left( \sum_{i=1}^n u_i(k) \right)^2 = 0,$$

which is equivalent to (44). $\square$

We are now ready to state the main theorem, the proof of which is reported in the appendix:

**Theorem 6.** *Suppose that* (44) *holds, then the disclosed space* $\mathbb{D}$ *contains the following subspaces:*

$$\mathbb{D} \supseteq \left\{ \begin{bmatrix} \tilde{\zeta} \\ 0 \end{bmatrix} \in \mathbb{R}^n : \tilde{\zeta} \in range(\mathcal{Q}_1) \right\} \oplus \{te_n : t \in \mathbb{R}\}. \tag{45}$$

**Remark 7.** *Comparing Theorem 6 with Theorem 4, we can see that the algorithm proposed in Section III achieves the minimum privacy "breach".*

## VI. Numerical Examples

We consider the following network consisted of 5 agents, whose topology is illustrated in Fig 1. We assume the following $A$ matrix is used:

$$A = \frac{1}{4}\begin{bmatrix} 2 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

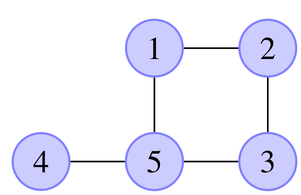


Fig. 1. Network Topology

We choose $\varphi = 0.9$. Fig 2 illustrates the trajectory of $x_i(k)$. It is worth noticing that all $x_i(k)$s converge to the true average of the initial condition $x(0)$.

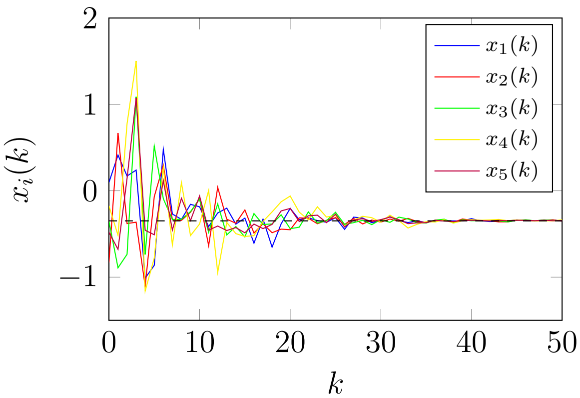


Fig. 2. The trajectory of each state $x_i(k)$. The blue, red, green, yellow and purple lines correspond to $x_1(k), x_2(k), x_3(k), x_4(k), x_5(k)$ respectively. The black dashed line corresponds to the average value of the initial $x(0)$.

Next, we implement the privacy preserving consensus protocol proposed by Huang et al. [15], by using independent and exponentially decaying Laplacian noise as our $w(k)$. To be specific, we assume that the probability density function of $w_i(k)$ is given by

$$\text{PDF}(w_i(k)) = \frac{1}{2b(k)} \exp\left(-\frac{|w_i(k)|}{b(k)}\right),$$

where $b(k) = \varphi^k$. From Fig 3, it can be seen that although consensus is achieved, the final result is not the original average, which may not be desirable for certain applications. However, it is worth noticing that Huang's algorithm can potentially provide more privacy guarantees due to the fact that it does not require consensus on the exact average. For the example discussed in this section, Huang's algorithm can preserve the privacy of agent $4$. On the other hand, we prove in Section V that the initial condition of the agent $4$ will be leaked to agent $5$ if we want to achieve average consensus. Therefore, there is a trade-off between privacy and the accuracy of the consensus.

Finally, Fig 4 shows $P_{ii}(k)$ of the maximum likelihood estimate of agent $4$ and the asymptotic $P_{ii}$ derived by Theorem 3. $P_{33}(k)$ is omitted since it equals $P_{11}(k)$ due to symmetry. Notice that both $P_{11}$ and $P_{22}$ are greater than $0$. As a result, agent $5$ cannot infer the exact initial condition of agent $1$ or agent $2$. On the other hand, $P_{44} = 0$. Therefore, the initial condition of agent $4$ is not private to agent $5$. One can easily check that

$$\mathcal{N}_e(4) \cup \{4\} = \{4, 5\} \subset \mathcal{N}(5) \cup \{5\} = \{1, 3, 4, 5\}.$$

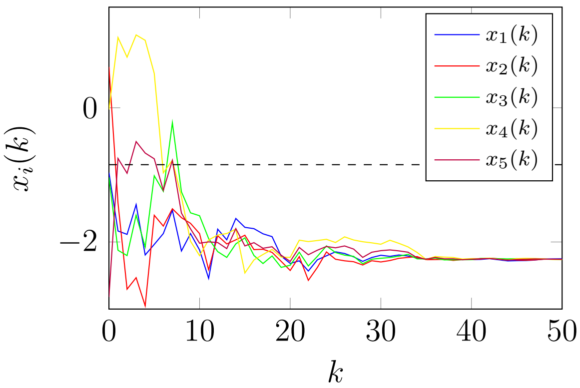


Fig. 3. The trajectory of each state $x_i(k)$ when using the privacy preserving consensus protocol proposed by Huang et al. [15]. The blue, red, green, yellow and purple lines correspond to $x_1(k), x_2(k), x_3(k), x_4(k), x_5(k)$ respectively. The black dashed line corresponds to the average value of the initial $x(0)$.

Hence, by Corollary 1, $e_4$ is in the disclosed space.

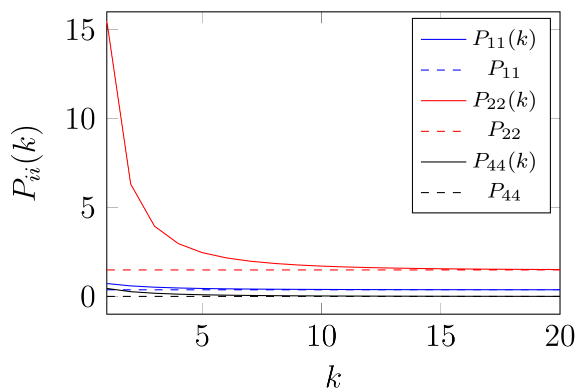


Fig. 4. $P_{ii}(k)$ v.s. $k$. The blue solid and dashed line correspond to $P_{11}(k)$ and $P_{11}$ respectively. The red solid and dashed line correspond to $P_{22}(k)$ and $P_{22}$ respectively. The black solid and dashed line correspond to $P_{44}(k)$ and $P_{44}$ respectively.

## VII. Conclusion and Future Work

In this paper, we propose a privacy preserving average consensus algorithm. We compute the exact mean square convergence rate of the proposed algorithm and characterize the covariance matrix of the maximum likelihood estimate, which guarantees the privacy of the initial condition. Moreover, we consider a general consensus framework and derive a fundamental limit for all average consensus algorithms and prove that our proposed algorithm achieves minimum privacy breach. Future work includes investigating other types of consensus problems, such as finite step consensus, binary consensus or consensus on network with time-varying topology, and designing algorithms that preserve the privacy of the participating agents.

## APPENDIX A
## PROOF OF LEMMA 2

*Proof.* Denote the eigenvalues of $\tilde{A}$ as $\tilde{\lambda}_1 \geq \tilde{\lambda}_2 \geq \cdots \geq \tilde{\lambda}_{n-1}$. By Cauchy's Interlace Theorem [19], we have

$$-1 < \lambda_n \leq \tilde{\lambda}_{n-1} \leq \lambda_{n-1} \leq \cdots \leq \lambda_2 \leq \tilde{\lambda}_1 \leq \lambda_1 = 1.$$

Hence, we only need to prove that $\tilde{\lambda}_1 \neq 1$. Suppose the opposite. Let $\|\xi\|_2 = 1$ be the eigenvector corresponding to $\tilde{\lambda}_1$. Hence,

$$A \begin{bmatrix} \xi \\ 0 \end{bmatrix} = \begin{bmatrix} \tilde{A}\xi \\ \eta'\xi \end{bmatrix} = \begin{bmatrix} \xi \\ \eta'\xi \end{bmatrix}.$$

Since $\|A\| = 1$, the 2-norm of the RHS is no greater than 1, which implies that $\eta'\xi = 0$. As a result, $\begin{bmatrix} \xi' & 0 \end{bmatrix}'$ is also an eigenvector of $A$ corresponding to eigenvalue 1, which contradicts with Assumption (A1) and (A2). As a result, $\|\tilde{A}\| < 1$. Hence, $I - \tilde{A} > 0$, which implies that $\tilde{A}_{ii} < 1$. □

## APPENDIX B
## PROOF OF THEOREM 2

One intermediate result is needed before proving Theorem 2. First define

$$x_r(k) \triangleq \begin{bmatrix} x_1(k) & \ldots & x_{n-1}(k) \end{bmatrix}' \in \mathbb{R}^{n-1}.$$

The following lemma characterize the relation between $x_r(k)$ and $\tilde{x}(k)$.

**Lemma 3.** $x_r(k+1) - \tilde{x}(k+1) = \sum_{t=0}^{k} \tilde{A}^{k-t}\eta x_n^+(t), \forall k \geq 0.$

*Proof.* The lemma can be proved by the fact that

$$x_r(k+1) = \tilde{A}(x_r(k) + \tilde{w}(k)) + \eta x_n^+(k),$$

and $x_r(0) = \tilde{x}(0)$. □

We are now ready to prove Theorem 2.

*Proof of Theorem 2.* We will prove Theorem 2 by induction. First consider the case where $k = 0$. By (26),

$$y(0)' = \begin{bmatrix}\tilde{y}(0)' & x_n(0) + w_n(0)\end{bmatrix}.$$

Hence, Theorem 2 holds when $k = 0$. Suppose that Theorem 2 holds when $k = t$, we want to prove that it still holds when $k = t + 1$. By induction assumption, we only need to prove that

1) $w_n(t + 1)$ and $\tilde{y}(t + 1)$ can both be written as linear combinations of the variables in $\mathcal{I}(t + 1)$.
2) $y(t + 1)$ can be written as a linear combination of the variables in $\tilde{\mathcal{I}}(t + 1)$.

It is easy to verify that

$$y(t+1) - \begin{bmatrix}\tilde{y}(t+1) \\ w_n(t+1)\end{bmatrix} = \begin{bmatrix}\tilde{C}(x_r(t+1) - \tilde{x}(t+1)) \\ x_n(t+1)\end{bmatrix}.$$

By Lemma 3 and (10), the RHS can be written as a linear combination of the variables in $\mathcal{I}(t)$ and hence a linear combination of the variables in $\tilde{\mathcal{I}}(t)$ by the induction assumption, which finishes the proof. $\square$

## Appendix C
## Proof of Theorem 3

We first try to explicitly write down the relationship between $\tilde{x}(0)$ and $\tilde{y}(k)$. By definition,

$$\tilde{y}(k) = \tilde{C}\left(\tilde{A}^k\tilde{x}(0) + \sum_{t=0}^{k}\tilde{A}^{k-t}\tilde{w}(t)\right). \tag{46}$$

We want to replace $\tilde{w}(t)$ in (46) with $\tilde{v}(t)$ since $\{\tilde{v}(t)\}_t$ is uncorrelated. As a result, we have

$$\sum_{t=0}^{k}\tilde{y}(t) = \tilde{C}(I - \tilde{A}^{k+1})(I - \tilde{A})^{-1}\tilde{x}(0) + \tilde{C}\sum_{t=0}^{k}\tilde{A}^{k-t}\varphi^t\tilde{v}(t), \tag{47}$$

which implies that

$$\begin{bmatrix}\sum_{t=0}^{0}\tilde{y}(t)/\varphi^0 \\ \sum_{t=0}^{1}\tilde{y}(t)/\varphi^1 \\ \vdots \\ \sum_{t=0}^{k}\tilde{y}(t)/\varphi^k\end{bmatrix} = H(k)\tilde{x}(0) + F(k)\begin{bmatrix}\tilde{v}(0) \\ \tilde{v}(1) \\ \vdots \\ \tilde{v}(k)\end{bmatrix}, \tag{48}$$

where

$$H(k) \triangleq \begin{bmatrix} \tilde{C}(I-\tilde{A})^{-1}/\varphi^0 \\ \tilde{C}(I-\tilde{A})^{-1}/\varphi^1 \\ \vdots \\ \tilde{C}(I-\tilde{A})^{-1}/\varphi^k \end{bmatrix} - \begin{bmatrix} \tilde{C}\tilde{A}(\tilde{A}/\varphi)^0(I-\tilde{A})^{-1} \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^1(I-\tilde{A})^{-1} \\ \vdots \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^k(I-\tilde{A})^{-1} \end{bmatrix}, \tag{49}$$

and

$$F(k) \triangleq \begin{bmatrix} \tilde{C} & & & \\ \tilde{C}\tilde{A}/\varphi & \tilde{C} & & \\ \vdots & \vdots & \ddots & \\ \tilde{C}(\tilde{A}/\varphi)^k & \tilde{C}(\tilde{A}/\varphi)^{k-1} & \dots & \tilde{C} \end{bmatrix}. \tag{50}$$

To simplify notations, let us define

$$H_1(k) \triangleq \begin{bmatrix} \varphi^0 I \\ \vdots \\ \varphi^{-k} I \end{bmatrix} \tilde{C}(I-\tilde{A})^{-1}, \tag{51}$$

$$\mathcal{H}(k) \triangleq \begin{bmatrix} \tilde{C}\tilde{A}(\tilde{A}/\varphi)^0 \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^1 \\ \vdots \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^k \end{bmatrix}, H_2(k) \triangleq \mathcal{H}(k)(I-\tilde{A})^{-1}. \tag{52}$$

Therefore $H(k) = H_1(k) - H_2(k)$. The covariance $\tilde{P}(k)$ of the maximum likelihood estimate [20] is given by

$$\tilde{P}(k) = \left[H(k)'(F(k)F(k)')^{-1}H(k)\right]^{-1}. \tag{53}$$

Consider the following matrix

$$\mathcal{S}(k) \triangleq \mathcal{Q}'H(k)'(F(k)F(k)')^{-1}H(k)\mathcal{Q} = \begin{bmatrix} \mathcal{S}_{11}(k) & \mathcal{S}_{12}(k) \\ \mathcal{S}_{12}'(k) & \mathcal{S}_{22}(k) \end{bmatrix},$$

where

$$\mathcal{S}_{11}(k) = \mathcal{Q}_1'H(k)'(F(k)F(k)')^{-1}H(k)\mathcal{Q}_1,$$

$$\mathcal{S}_{22}(k) = \mathcal{Q}_2'H(k)'(F(k)F(k)')^{-1}H(k)\mathcal{Q}_2,$$

$$\mathcal{S}_{12}(k) = \mathcal{Q}_1'H(k)'(F(k)F(k)')^{-1}H(k)\mathcal{Q}_2,$$

and $\mathcal{Q}$ is defined in (29). We know that

$$\tilde{P}(k) = \mathcal{Q} \begin{bmatrix} \mathcal{S}_{11}(k) & \mathcal{S}_{12}(k) \\ \mathcal{S}'_{12}(k) & \mathcal{S}_{22}(k) \end{bmatrix}^{-1} \mathcal{Q}'.$$

The rest of the proof will be divided into 3 steps:

1) We prove that for any $M > 0$, we have $\mathcal{S}_{11}(k) > MI$ if $k$ is large enough.
2) We prove that $S_{22}(k)$ converges to a unique positive definite matrix.
3) We derive $\tilde{P}(k)$ using the above two intermediate results and the fact that $\tilde{P}(k)$ is non-increasing.

*Step 1:* $\mathcal{S}_{11}(k) \to \infty$

To prove that for any $M > 0$, there exists a $k$, such that $\mathcal{S}_{11}(k) \geq MI$, we first need the following lemma:

**Lemma 4.** *Assume that* $X = \begin{bmatrix} X_{11} & X_{12} \\ X'_{12} & X_{22} \end{bmatrix}$ *is strictly positive definite, then the following inequality holds*

$$\begin{bmatrix} V_1 \\ V_2 \end{bmatrix}' X^{-1} \begin{bmatrix} V_1 \\ V_2 \end{bmatrix} \geq V'_1 X_{11}^{-1} V_1, \tag{54}$$

*where* $V_1$ *and* $V_2$ *are matrices of proper dimension.*

*Proof.* Using the Schur complement, we can write $X^{-1}$ as

$$X^{-1} = \begin{bmatrix} X_{11}^{-1} & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} X_{11}^{-1} X_{12} \\ I \end{bmatrix} (X_{22} - X'_{12} X_{11}^{-1} X_{12})^{-1} \begin{bmatrix} X'_{12} X_{11}^{-1} & I \end{bmatrix},$$

which immediately implies (54). □

We are now ready to prove the main result for this subsection:

**Lemma 5.** *For any* $M > 0$*, there exists a* $k$*, such that* $\mathcal{S}_{11}(k) \geq MI$*.*

*Proof.* Let us define

$$h(k) = \tilde{C}(I - \tilde{A})^{-1}\left[\varphi^{-k}I - \tilde{A}(\tilde{A}/\varphi)^k\right].$$

By definition, we know that

$$H(k) = \begin{bmatrix} h(0) \\ \vdots \\ h(k) \end{bmatrix}.$$

Hence, by Lemma 4, we know that

$$\begin{aligned}\mathcal{S}_{11}(k) &\geq \mathcal{Q}_1' h(k)' \left(\tilde{C}\sum_{t=0}^{k}(\tilde{A}/\varphi)^{2t}\tilde{C}'\right)^{-1} h(k)\mathcal{Q}_1 \\ &= \mathcal{Q}_1'(\varphi^k h(k))' \left(\tilde{C}\sum_{t=0}^{k}\tilde{A}^{2t}\varphi^{2k-2t}\tilde{C}'\right)^{-1} \varphi^k h(k)\mathcal{Q}_1.\end{aligned}$$

Since both $\tilde{A}$ and $\varphi$ are stable, we have

$$\tilde{A}^{2t}\varphi^{2k-2t} \leq \tilde{\rho}^k I, \forall 0 \leq t \leq k,$$

where $\tilde{\rho} = \max(\varphi^2, \|\tilde{A}\|^2) < 1$. Therefore,

$$\tilde{C}\sum_{t=0}^{k}\tilde{A}^{2t}\varphi^{2k-2t}\tilde{C}' \leq k\tilde{\rho}^k\tilde{C}\tilde{C}' = k\tilde{\rho}^k I.$$

Thus,

$$\mathcal{S}_{11}(k) \geq \frac{\tilde{\rho}^{-k}}{k}(\varphi^k h(k)\mathcal{Q}_1)'(\varphi^k h(k)\mathcal{Q}_1). \tag{55}$$

Since $\varphi^k h(k)\mathcal{Q}_1$ converges to $\tilde{C}(I - \tilde{A})^{-1}\mathcal{Q}_1$, by the definition of $\mathcal{Q}_1$,

$$\begin{aligned}&\lim_{k\to\infty}(\varphi^k h(k)\mathcal{Q}_1)'(\varphi^k h(k)\mathcal{Q}_1) \\ &\quad = \mathcal{Q}_1'(I - \tilde{A})^{-1}\tilde{C}'\tilde{C}(I - \tilde{A})^{-1}\mathcal{Q}_1 > 0,\end{aligned}$$

which concludes the proof. □

*Step 2: Convergence of $\mathcal{S}_{22}(k)$*

We now prove that

$$\lim_{k\to\infty} \mathcal{S}_{22}(k) = \mathcal{Q}_2'(I-\tilde{A})^{-1}Y(I-\tilde{A})^{-1}\mathcal{Q}_2 > 0, \tag{56}$$

which requires the following lemmas:

**Lemma 6.** $\{Y(k)\}$ *matrices satisfy the following equality:*

$$Y(k) = \mathcal{H}(k)'\left(F(k)F(k)'\right)^{-1}\mathcal{H}(k) \tag{57}$$

*Proof.* We prove (57) by induction. Since $F(0)F(0)' = \tilde{C}\tilde{C}' = I$, it is clear that (57) holds when $k = 0$. Now assume that (57) holds for $k$. We need to prove that

$$Y(k+1) = \mathcal{H}(k+1)'\left(F(k+1)F(k+1)'\right)^{-1}\mathcal{H}(k+1) \tag{58}$$

By the definition of the matrix $F(k)$ and $\mathcal{H}(k)$, we know that

$$F(k+1) = \begin{bmatrix} & \tilde{C} & \\ \varphi^{-1}\mathcal{H}(k) & & F(k) \end{bmatrix},$$

and

$$\mathcal{H}(k+1) = \begin{bmatrix} \varphi\tilde{C} \\ \mathcal{H}(k) \end{bmatrix}\tilde{A}/\varphi.$$

As a result, the following equality holds:

$$\begin{aligned} &\left(F(k+1)F'(k+1)\right)^{-1} \\ &= \begin{bmatrix} I & \tilde{C}\mathcal{H}(k)'/\varphi \\ \mathcal{H}(k)\tilde{C}'/\varphi & \mathcal{H}(k)\mathcal{H}(k)'/\varphi^2 + F(k)F(k)' \end{bmatrix}^{-1} \\ &= \begin{bmatrix} I + \tilde{C}\mathcal{H}(k)'Z(k)\mathcal{H}(k)\tilde{C}'/\varphi^2 & -\tilde{C}\mathcal{H}(k)'Z(k)/\varphi \\ -Z(k)\mathcal{H}(k)\tilde{C}'/\varphi & Z(k) \end{bmatrix}, \end{aligned} \tag{59}$$

where

$$Z(k) = \left[F(k)F(k)' + \varphi^{-2}\mathcal{H}(k)\mathcal{V}\mathcal{H}(k)'\right]^{-1} \tag{60}$$

The first equality of (59) holds since $\tilde{C}\tilde{C}' = I$. The second equality holds due to the matrix inversion lemma. Using (59), the RHS of (58) can be simplified as

$$\text{RHS} = \varphi^{-2}\tilde{A}(\varphi^2\mathcal{U} + \mathcal{V}\mathcal{H}(k)'Z(k)\mathcal{H}(k)\mathcal{V})\tilde{A} \tag{61}$$

Since $\mathcal{V}$ is a projection matrix, by the matrix inversion lemma

$$\begin{aligned} Z(k) &= \left[F(k)F(k)' + \varphi^{-2}\mathcal{H}(k)\mathcal{V}\mathcal{V}\mathcal{H}(k)'\right]^{-1} \\ &= (F(k)F(k)')^{-1} - Z_1(k)Z_2(k)Z_1(k)' \end{aligned} \tag{62}$$

where

$$\begin{aligned} Z_1(k) &= (F(k)F(k)')^{-1}\,\mathcal{H}(k)\mathcal{V}, \\ Z_2(k) &= \left[\varphi^2 I + \mathcal{V}\mathcal{H}(k)'\,(F(k)F(k)')^{-1}\,\mathcal{H}(k)\mathcal{V}\right]^{-1}. \end{aligned}$$

Now by the induction assumption, (35), (61) and (62), the RHS of (58) can be rewritten as

$$\begin{aligned} \text{RHS} &= \tilde{A}\mathcal{U}\tilde{A} \\ &+ \varphi^{-2}\tilde{A}\left[Y^+(k) - Y^+(k)\left(\varphi^2 I + Y^+(k)\right)^{-1} Y^+(k)\right]\tilde{A} \\ &= Y(k+1). \end{aligned}$$

Thus, (57) holds for all $k$ by induction. □

**Lemma 7.** *The following statements on the $\{Y(k)\}$ matrices defined recursively in* (35) *and* (34) *hold:*

1) *$Y(k)$ is non-decreasing in $k$.*
2) *The limit $Y = \lim_{k\to\infty} Y(k)$ is well-defined.*
3) *$Y + \mathcal{U} > 0$ is strictly positive definite.*

*Proof.* Let us define the following function for positive semidefinite matrices:

$$g(X) \triangleq X - X(\varphi^2 I + X)^{-1}X.$$

For any matrix $K$ of proper dimension, it can be verified that

$$\varphi^2 KK' + (I+K)X(I+K)' = (K - K^*)(\varphi^2 I + X)(K - K^*)' + g(X),$$

where $K^* = -X(\varphi^2 I + X)^{-1}$. Therefore, $g(X)$ can be written as the solution of the following optimization problem:

$$g(X) = \arg\min_K \ \varphi^2 KK' + (I+K)X(I+K)'.$$

If $X \geq 0$ is positive semidefinite, then the RHS $\geq 0$ for all $K$ matrices. Hence we can conclude that $g(X) \geq 0$ if $X \geq 0$. Furthermore, by Lemma 1(c) in [21], $g(X)$ is non-decreasing in $X$.

On the other hand, we could perform an eigen-decomposition on $X$, i.e.,

$$X = Q\Lambda Q^T,$$

where $Q$ is an orthogonal matrix and $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_{n-1}) \geq 0$ is diagonal. Therefore, $g(X)$ can be rewritten as

$$g(X) = Q\text{diag}\left(\frac{\varphi^2\lambda_1}{\varphi^2+\lambda_1}, \dots, \frac{\varphi^2\lambda_{n-1}}{\varphi^2+\lambda_{n-1}}\right)Q^T.$$

Hence, we can conclude that for any $X \geq 0$,

1) $g(X) \leq \varphi^2 I$,
2) and $\text{null}(g(X)) = \text{null}(X)$.

We now prove that $Y(k)$ is non-decreasing in $k$ by induction. Manipulating (34), we have

$$Y(1) = \tilde{A}\mathcal{U}\tilde{A} + \varphi^{-2}\tilde{A}g(Y^+(0))\tilde{A} \geq \tilde{A}\mathcal{U}\tilde{A} = Y(0),$$

where we use the fact that $g(Y^+(0)) \geq 0$. Now suppose that $Y(k) \geq Y(k-1)$. By (35), $Y^+(k) \geq Y^+(k-1)$. By the fact that the function $g$ is non-decreasing, $Y(k+1) \geq Y(k)$. Therefore, by induction, $Y(k)$ is non-decreasing.

Next we prove that $Y(k)$ converges to a matrix $Y$. Since $g(X) \leq \varphi^2 I$, we know that

$$Y(k+1) = \tilde{A}\mathcal{U}\tilde{A} + \varphi^{-2}\tilde{A}g(Y^+(k))\tilde{A} \leq \tilde{A}(\mathcal{U}+I)\tilde{A}.$$

Thus, $Y(k)$ is non-decreasing and bounded, which implies that the limit $Y = \lim_{k\to\infty} Y(k)$ is well-defined.

Finally we prove that $Y + \mathcal{U}$ is strictly positive. We first prove that for any $X \geq 0$

$$\text{null}(\mathcal{U} + \varphi^{-2}g(\mathcal{V}X\mathcal{V})) \subseteq \text{null}(\mathcal{U}) \cap \text{null}(X). \tag{63}$$

Assuming that $v \in \text{null}(\mathcal{U} + \varphi^{-2}g(\mathcal{V}X\mathcal{V}))$. By the fact that $\mathcal{U}$ and $X$ are positive semidefinite, we know that

$$v'\mathcal{U}v + \varphi^{-2}v'g(\mathcal{V}X\mathcal{V}))v = 0,$$

which implies that $v'\mathcal{U}v = 0$ and $v'\mathcal{V}X\mathcal{V}v = 0$ since $\mathrm{null}(g(\mathcal{V}X\mathcal{V})) = \mathrm{null}(\mathcal{V}X\mathcal{V})$. Moreover $\mathcal{U}v = 0$. Now since $\mathcal{U} + \mathcal{V} = I$, $\mathcal{V}v = v$, which further implies that $v'Xv = 0$. Thus, $v'Xv = 0 = v'\mathcal{U}v$, which proves (63).

By induction and (63), we can prove that

$$\mathrm{null}(Y(k)) \subseteq \mathrm{null}(\tilde{A}\mathcal{U}\tilde{A}) \cap \cdots \cap \mathrm{null}(\tilde{A}^{k+1}\mathcal{U}\tilde{A}^{k+1}).$$

As a result, by the fact that both $Y(k)$ and $\mathcal{U}$ are positive semidefinite,

$$\mathrm{null}(Y(k) + \mathcal{U}) \subseteq \mathrm{null}(\tilde{A}\mathcal{U}\tilde{A}) \cap \cdots \cap \mathrm{null}(\tilde{A}^{k+1}\mathcal{U}\tilde{A}^{k+1}) \cap \mathrm{null}(\mathcal{U}).$$

By the assumption that $(\tilde{A}, \tilde{C})$ is observable, we know that $Y + \mathcal{U} > 0$ is strictly positive definite.

□

By the definition of $\mathcal{Q}_2$, we know that

$$\mathcal{Q}_2'(I - \tilde{A})^{-1}\tilde{C}'\tilde{C}(I - \tilde{A})^{-1}\mathcal{Q}_2 = 0.$$

Hence, $H_1(k)\mathcal{Q}_2 = 0$ and

$$H(k)\mathcal{Q}_2 = H_2(k)\mathcal{Q}_2 = \mathcal{H}(k)(I - \tilde{A})^{-1}\mathcal{Q}_2,$$

which, combined with Lemma 6, proves the first equality in (56). Notice that $\mathcal{Q}_2'(I-\tilde{A})^{-1}\mathcal{U}(I-\tilde{A})^{-1}\mathcal{Q}_2 = 0$, we know that

$$\begin{aligned}\lim_{k\to\infty} \mathcal{S}_{22}(k) &= \mathcal{Q}_2'(I - \tilde{A})^{-1}Y(I - \tilde{A})^{-1}\mathcal{Q}_2 \\ &= \mathcal{Q}_2'(I - \tilde{A})^{-1}(Y + \mathcal{U})(I - \tilde{A})^{-1}\mathcal{Q}_2 > 0.\end{aligned}$$

*Step 3: Proof of Theorem 3*

We now prove Theorem 3 using Lemma 5 and (56). Before proving the main theorem, we need the following lemma:

**Lemma 8.** *Let $\{S(k)\}_{k=0,1,\dots}$ be an infinite non-deceasing sequence of positive semidefinite matrices, i.e.,*

$$0 \le S(0) \le S(1) \le \cdots \le S(k) \le \dots$$

*Assume that $S(k)$ can be written in a block diagonal form*

$$S(k) = \begin{bmatrix} S_{11}(k) & S_{12}(k) \\ S_{12}(k)' & S_{22}(k) \end{bmatrix},$$

*and the following conditions hold:*

1) $S_{22}(k)$ *converges to a strictly positive definite matrix, i.e.,* $\lim_{k\to\infty} S_{22}(k) = S_{22} > 0$*;*
2) *For any* $M > 0$*, there exists a* $k$*, such that* $S_{11}(k) > MI$*.*

*Then there exists an* $N$*, such that for all* $k \geq N$*,* $S(k)$ *is strictly positive definite (and hence invertible). Furthermore,*

$$\lim_{k\to\infty} (S(k))^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & S_{22}^{-1} \end{bmatrix}. \tag{64}$$

*Proof.* From the assumptions, we know that there exists an $N_1$, such that $S_{11}(k)$, $S_{22}(k)$ are all strictly positive definite if $k \geq N_1$. We will first prove the following limits:

$$\lim_{k\to\infty} S_{21}(k) \left(S_{11}(k)\right)^{-1} S_{12}(k) = 0 \tag{65}$$

For any $\epsilon > 0$, let us choose $N_2 \geq N_1$, such that $S_{22}(k) \geq S_{22} - \epsilon I$, for all $k \geq N_2$. As a result, if $k \geq N_2$, then we have

$$\begin{aligned} & S_{21}(k) \left(S_{11}(k)\right)^{-1} S_{12}(k) \\ & \leq 2S_{21}(N_2) \left(S_{11}(k)\right)^{-1} S_{12}(N_2) \\ & + 2 \left(S_{21}(k) - S_{21}(N_2)\right) \left(S_{11}(k)\right)^{-1} \left(S_{12}(k) - S_{12}(N_2)\right). \end{aligned} \tag{66}$$

Since for any $M \geq 0$, $S_{11}(k) \geq MI$ when $k$ is large enough, we can find an $N_3 \geq N_2$, such that for all $k \geq N_3$,

$$S_{21}(N_2) \left(S_{11}(k)\right)^{-1} S_{12}(N_2) \leq \epsilon I. \tag{67}$$

For the second term on the RHS of (66), since $S(k)$ is non-decreasing, we know that $S(k) - S(N_2) \geq 0$, which implies that for any $k \geq N_2$

$$\begin{aligned} \epsilon I &\geq S_{22} - S_{22}(N_2) \geq S_{22}(k) - S_{22}(N_2) \\ &\geq \left(S_{21}(k) - S_{21}(N_2)\right) \left(S_{11}(k)\right)^{-1} \left(S_{12}(k) - S_{12}(N_2)\right), \end{aligned}$$

where the last inequality is due to Schur complement and the fact that $S_{11}(k) \geq S_{11}(k)-S_{11}(N_2)$. Therefore, for any $k \geq N_2$,

$$\left(S_{21}(k)-S_{21}(N_2)\right)\left(S_{11}(k)\right)^{-1}\left(S_{12}(k)-S_{12}(N_2)\right) \leq \epsilon I. \tag{68}$$

Combining (67) and (68), we know that for any $k \geq N_3$,

$$S_{21}(k)\left(S_{11}(k)\right)^{-1} S_{12}(k) \leq 4\epsilon I.$$

Therefore, (65) holds, which further implies that

$$\lim_{k\to\infty} S_{22}(k) - S_{21}(k)\left(S_{11}(k)\right)^{-1} S_{12}(k) = S_{22} > 0. \tag{69}$$

As a result, when $k$ is large enough, $S(k)$ is strictly positive definite.

Next we want to prove the following equality:

$$\lim_{k\to\infty} \left[S_{11}(k) - S_{12}(k)\left(S_{22}(k)\right)^{-1} S_{21}(k)\right]^{-1} = 0 \tag{70}$$

Let us rewrite (65) as

$$\lim_{k\to\infty} \operatorname{tr}\left(S_{21}(k)\left(S_{11}(k)\right)^{-1} S_{12}(k)\right) = 0. \tag{71}$$

Let $\left(S_{11}(k)\right)^{-1/2}$ be a positive definite matrix such that

$$\left(S_{11}(k)\right)^{-1/2}\left(S_{11}(k)\right)^{-1/2} = \left(S_{11}(k)\right)^{-1}.$$

Using the properties of the trace operator, (71) can be written as,

$$\lim_{k\to\infty} \operatorname{tr}\left(\left(S_{11}(k)\right)^{-1/2} S_{12}(k)S_{21}(k)\left(S_{11}(k)\right)^{-1/2}\right) = 0,$$

which means for any $\epsilon > 0$, we can find an $N$, such that for all $k \geq N$, we have

$$\left(S_{11}(k)\right)^{-1/2} S_{12}(k)S_{21}(k)\left(S_{11}(k)\right)^{-1/2} \leq \epsilon I,$$

which is equivalent to

$$S_{12}(k)S_{21}(k) \leq \epsilon S_{11}(k).$$

Since $S_{22}(k)$ converges to $S_{22} > 0$, we can prove that for large enough $k$, the following inequality holds

$$S_{12}(k)\left(S_{22}(k)\right)^{-1} S_{21}(k) \leq 0.5 S_{11}(k).$$

Combining with the fact that for any $M > 0$ $S_{11}(k) > MI$ if $k$ is large enough, we can prove (70). Equation (64) is a direct consequence of (69), (70) and the fact that the inverse of $S$ is positive semidefinite. □

We are now ready to prove Theorem 3:

*Proof.* By Proposition 1, $\mathcal{S}(k)$ is monotonically non-decreasing. Hence, by Lemma 5, (56) and Lemma 8, we know that

$$\lim_{k\to\infty} \mathcal{S}(k)^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & \left(\mathcal{Q}_2'(I-\tilde{A})^{-1}Y(I-\tilde{A})^{-1}\mathcal{Q}_2\right)^{-1} \end{bmatrix}.$$

Use the fact that $\tilde{P} = \lim_{k\to\infty} \mathcal{Q}'\mathcal{S}(k)^{-1}\mathcal{Q}$, we can conclude the proof. □

## Appendix D
## Proof of Theorem 6

The following lemma is needed to prove Theorem 6.

**Lemma 9.** *Suppose that a non-negative sequence $\{a(k)\}$ satisfies*

$$\lim_{k\to\infty} a(k) = 0,$$

*then for any $0 < \lambda < 1$, the following equality holds*

$$\lim_{k\to\infty} \left(\sum_{t=0}^{k} \lambda^t \sqrt{a(k-t)}\right)^2 = 0.$$

*Proof.* Since $a(k)$ converges to $0$, there exists $M > 0$, such that $\sqrt{a(k)} < M$ for all $k$. For any $\varepsilon > 0$, there exists an $N_1$, such that for all $k \geq N_1$,

$$\left(\sum_{t=N_1}^{k} \lambda^t \sqrt{a(k-t)}\right)^2 \leq \left(M \sum_{t=N_1}^{\infty} \lambda^t\right)^2 \leq \varepsilon/4.$$

On the other hand, since $a(k)$ converges to $0$, there exists an $N_2 \geq N_1$, such that for any $k > N_2$

$$\left(\sum_{t=0}^{N_1-1} \lambda^t \sqrt{a(k-t)}\right)^2 \leq \varepsilon/4,$$

which implies that

$$
\begin{aligned}
&\left(\sum_{t=0}^{k}\lambda^t\sqrt{a(k-t)}\right)^2\\
&=\left(\sum_{t=0}^{N_1-1}\lambda^t\sqrt{a(k-t)}+\sum_{t=N_1}^{k}\lambda^t\sqrt{a(k-t)}\right)^2\\
&\leq 2\left(\sum_{t=0}^{N_1-1}\lambda^t\sqrt{a(k-t)}\right)^2+2\left(\sum_{t=N_1}^{k}\lambda^t\sqrt{a(k-t)}\right)^2\leq\varepsilon,
\end{aligned}
$$

which finishes the proof. □

We are now ready to prove Theorem 6.

*Proof.* Since $x_n(0)\in\mathcal{I}(k)$, it is clear that $e_n\in\mathbb{D}$. Now consider the vector $\sum_{t=0}^{k}\tilde{y}(t)$, which is a function of $\mathcal{I}(k)$ by Theorem 2. One can easily prove that

$$
\sum_{t=0}^{k}\tilde{y}(t)=\tilde{C}\sum_{t=0}^{k}\tilde{A}^t\tilde{x}(0)+\sum_{t=0}^{k}\tilde{A}^{k-t}\tilde{u}(t),
$$

where $\tilde{u}(k)\triangleq\begin{bmatrix}u_1(k)&\dots&u_{n-1}(k)\end{bmatrix}'\in\mathbb{R}^{n-1}$. Therefore

$$
\begin{aligned}
&\mathbb{E}\|\sum_{t=0}^{k}\tilde{y}(t)-\tilde{C}(I-\tilde{A})^{-1}\tilde{x}(0)\|^2\\
&\quad=\|\tilde{C}\tilde{A}^{k+1}(I-\tilde{A})^{-1}x(0)\|^2+\mathbb{E}\|\sum_{t=0}^{k}\tilde{A}^{k-t}\tilde{u}(t)\|^2.
\end{aligned}
\tag{72}
$$

By Lemma 2, the first term on the RHS of (72) converges to $0$ as $k\to\infty$. On the other hand, by Cauchy-Schwarz inequality, we have

$$
\begin{aligned}
\mathbb{E}\|\sum_{t=0}^{k}\tilde{A}^{k-t}\tilde{u}(t)\|^2&\leq\left(\sum_{t=0}^{k}\sqrt{\mathbb{E}\,\|\tilde{A}^{k-t}\tilde{u}(t)\|^2}\right)^2\\
&\leq\left(\sum_{t=0}^{k}\|\tilde{A}\|^{k-t}\sqrt{\mathbb{E}\,\|\tilde{u}(t)\|^2}\right)^2
\end{aligned}
$$

By (44) and Lemma 9, the second term on the RHS of (72) converges to $0$. Therefore,

$$
\lim_{k\to\infty}\mathbb{E}\|\sum_{t=0}^{k}\tilde{y}(t)-\tilde{C}(I-\tilde{A})^{-1}\tilde{x}(0)\|^2=0.
$$

Since the column space of $\mathcal{Q}_1$ coincides with the column space of $(I-\tilde{A})^{-1}\tilde{C}'$,

$$\left\{ \begin{bmatrix} \tilde{\zeta} \\ 0 \end{bmatrix} \in \mathbb{R}^n : \tilde{\zeta} \in \text{range}(\mathcal{Q}_1) \right\} \subset \mathbb{D}.$$

$\square$

## REFERENCES


[1] M. DeGroot, "Reaching a consensus," *Journal of the American Statistical Association*, vol. 69, no. 345, pp. 118–121, March 1974.

[2] J. Tsitsiklis, "Problems in decentralized decision making and computation," *Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge*, November 1984.

[3] G. Cybenko, "Dynamic load balancing for distributed memory multiprocessors," *Journal of parallel and distributed computing*, vol. 7, pp. 279–301, 1989.

[4] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on automatic control*, vol. 48, no. 6, pp. 988–1001, June 2003.

[5] W. Ren, R. Beard, and E. Atkins, "A survey of consensus problems in multi-agent coordination," in *American Control Conference*, June 2005, pp. 1859–1864.

[6] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, January 2007.

[7] A. G. Dimakis, S. Kar, J. M. F. Moura, M. G. Rabbat, and A. Scaglione, "Gossip algorithms for distributed signal processing," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1847–1864, November 2010.

[8] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on automatic control*, vol. 57, no. 1, pp. 90–104, 2012.

[9] S. Sundaram and C. Hadjicostis, "Finite-time distributed consensus in graphs with time-invariant topologies," in *American Control Conference*, 2007, pp. 711–716.

[10] Y. Yuan, G.-B. Stan, L. Shi, M. Barahona, and J. Goncalves, "Decentralised minimum-time consensus," *Automatica*, vol. 49, no. 5, pp. 1227 – 1235, 2013.

[11] J. Lin, A. S. Morse, and B. D. Anderson, "The multi-agent rendezvous problem," in *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, vol. 2. IEEE, 2003, pp. 1508–1513.

[12] C. Dwork, "Differential privacy," in *Automata, languages and programming*. Springer, 2006, pp. 1–12.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Springer, 2006, pp. 265–284.

[14] J. Le Ny and G. Pappas, "Differentially private filtering," *Automatic Control, IEEE Transactions on*, vol. 59, no. 2, pp. 341–354, Feb 2014.

[15] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 2012, pp. 81–90.

[16] N. Manitara and C. Hadjicostis, "Privacy-preserving asymptotic average consensus," in *Control Conference (ECC), 2013 European*, 2013, pp. 760–765. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6669251

[17] M. Xue, W. Wang, and S. Roy, "Security concepts for the dynamics of autonomous vehicle networks," *Automatica*, vol. 50, no. 3, pp. 852–857, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0005109813005608

[18] Y. Mo and R. M. Murray, “Privacy preserving average consensus,” in *the Proceedings of the 53rd CDC, to be appear*. IEEE, 2014. [Online]. Available: http://www.cds.caltech.edu/~murray/papers/2014d_mm14-cdc.html

[19] Y. Ikebe, T. Inagaki, and S. Miyamoto, “The monotonicity theorem, Cauchy’s interlace theorem, and the Courant- Fischer theorem,” *The American Mathematical Monthly*, vol. 94, no. 4, pp. 352–354, 1987.

[20] L. L. Scharf, *Statistical signal processing*. Addison-Wesley Reading, MA, 1991, vol. 98.

[21] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. Jordan, and S. Sastry, “Kalman filtering with intermittent observations,” *IEEE Transactions on automatic control*, vol. 49, no. 9, pp. 1453–1464, 2004.