Consensus Networks over Finite Fields

F. Pasqualetti [a], D. Borra [b], F. Bullo [a]

[a] *Center for Control, Dynamical Systems, and Computation, University of California, Santa Barbara, USA*

[b] *Dipartimento di Scienze Matematiche, Politecnico di Torino, Italy*

Abstract

This work studies consensus strategies for networks of agents with limited memory, computation, and communication capabilities. We assume that agents can process only values from a finite alphabet, and we adopt the framework of finite fields, where the alphabet consists of the integers $\{0, \dots, p-1\}$, for some prime number p, and operations are performed modulo p. Thus, we define a new class of consensus dynamics, which can be exploited in certain applications such as pose estimation in capacity and memory constrained sensor networks. For consensus networks over finite fields, we provide necessary and sufficient conditions on the network topology and weights to ensure convergence. We show that consensus networks over finite fields converge in finite time, a feature that can be hardly achieved over the field of real numbers. For the design of finite-field consensus networks, we propose a general design method, with high computational complexity, and a network composition rule to generate large consensus networks from smaller components. Finally, we discuss the application of finite-field consensus networks to distributed averaging and pose estimation in sensor networks.

1 Introduction

Sensor and actuator networks have recently attracted interest from different research communities and, in the last years, classic computation, control, and estimation problems have been reformulated to conform the distributed nature of these networked systems [1]. An important example is the *consensus* problem, where members of a network aim to agree upon a parameter of interest via distributed computation [2]. Consensus algorithms have applicability in many domains, including robotics [3], estimation [4], and parallel computation [5].

In this work we focus on the consensus problem for networks of agents with limited memory, computation, and communication capabilities. We assume that agents are capable of storing, processing, and transmitting exclusively elements from a finite and pre-specified alphabet. We model this situation with the formalism of *finite fields*, where the alphabet consists of a set of integers, and operations are performed according to modular arithmetic [6]. We study linear consensus networks over finite fields where, at each time instant, each agent updates its state as a weighted combination over a finite field of its own value and those received from its neighbors.

⋆ This work was supported by NSF grants IIS-0904501 and CNS-1035917, and by ARO grant W911NF-11-1-0092.

Email addresses: fabiopas@engineering.ucsb.edu (F. Pasqualetti), domenica.borra@polito.it (D. Borra), bullo@engineering.ucsb.edu (F. Bullo).

Besides consensus in capacity and memory constrained networks, our finite-field consensus method is applicable to problems in cooperative control, networked systems, and network coding, such as averaging, load balancing, and pose estimation from relative measurements. Additionally, the use of a finite alphabet for computation and communication makes our consensus method easily implementable and resilient to communication noise.

Related work Consensus algorithms have been developed for different network models, agents dynamics, and communication schemes. Starting from the basic setup of time-independent network structure, broadcast and synchronous communication, and unlimited communication bandwidth, consensus algorithms have been proposed to cope with time-varying topologies [7], gossip and asynchronous communication [8], and communication errors and link failures [9]. It has been shown that, under mild connectivity assumptions on the interaction graph, a simple linear iteration suffices to ensure consensus [10]. While most of these approaches assume the possibility of processing and transmitting real values, we consider the more realistic case of finite communication bandwidth, possibly due to digital communication and memory constraints. As we show, topological conditions ensuring consensus with real values and unlimited bandwidth are not sufficient for consensus over a finite field.

A relevant body of literature deals with consensus over *quantized* communication channels, where values exchanged by the agents are quantized according to a predefined quantization scheme, and the proposed al-

gorithms are resilient to quantization errors [11, 12]. In these works, although the exchanged data is quantized, agents perform real-valued computations. Thus, the consensus problem with quantized information is related to our problem, yet fundamentally different because we allow agents to operate only on a finite field.

Logical consensus has been studied in [13] for the purpose of intruder and event detection. In logical consensus agents aim to coordinate their decisions via distributed computation as a function of a set of logical (boolean) events. By leveraging tools from cellular automata and convergence theory of finite-state iteration maps, the focus of [13] is on the design of a synthesis technique for logical consensus systems. The main differences between [13] and this paper are as follows. First, in logical consensus the agents state is a binary variable, while in our work it takes value in an arbitrary finite set. Second, in logical consensus agents are allowed to perform any logical operation, such as $\{\text{and}, \text{or}, \text{not}\}$, as opposed to only modular addition and multiplication. Third and finally, in logical consensus agents aim to agree upon a logical expression or compact sets, while finite-field consensus algorithms may be used to compute a (non-boolean) function, such as the average of the initial states.

A distributed consensus algorithm with integer communication and computation is proposed in [14]. With respect to this work we make use of *modular arithmetic*, instead of standard arithmetic and, therefore, we define a novel and complementary class of consensus networks. The use of modular arithmetic is advantageous in several applications, such as pose estimation from relative measurements (Section 6). Finally, networks based on modular arithmetic are studied in [15], in the context of system controllability and observability, in [16], in the context of (linear) network coding, and in [17], in the more general context of finite dynamical systems.

Contributions The contributions of this paper are fourfold. First, we propose the use of finite fields to design consensus algorithms for networks of cooperative agents (Section 3). Finite-field consensus networks are distributed, require limited, in fact finite, memory, computation, and communication resources, and converge in finite time. Thus, finite-field consensus algorithms are suitable for capacity and memory constrained networks, and for applications subject to time constraints.

Second, we characterize convergence of consensus networks over finite fields (Section 4). We provide necessary and sufficient constructive conditions on the network topology and weights to achieve consensus. For instance, we show that a network achieves consensus over a finite field if and only if the network matrix is row-stochastic over the finite field, and its characteristic polynomial is $s^{n-1}(s-1)$. Additionally, we prove that the convergence time of finite-field consensus networks is bounded by the network cardinality, and that graph properties alone are not sufficient to ensure finite-field consensus.

Third, we propose systematic methods to design consensus networks over finite fields (Section 5). In particular, we derive a general design method, and a network composition rule based on graph products to generate large consensus networks from smaller components. We show that networks generated by our composition rule exhibit a specific structure, and maintain the convergence properties, including the convergence time, of the underlying components. Moreover, by using our general network design method we provide a lower bound on the number of networks achieving consensus as a function of the agents interaction graph and the field characteristic.

Fourth and finally, we consider two applications in sensor networks, namely averaging and pose estimation from relative measurements (Section 6). In the averaging problem agents aim to determine the average (over the field of real numbers) of their initial values. We show how, under a reasonable set of assumptions, the averaging problem can be solved distributively and in finite time via a finite-field average consensus. In the pose estimation problem agents aim to estimate their pose based on relative measurements. We derive a distributed pose estimation algorithm based on finite-field average consensus, and we characterize its performance.

2 Notation and Preliminary Concepts

In this section we recall some definitions and properties of algebraic fields, linear algebra, and graph theory. We refer the interested reader to [6, 18, 19] for a comprehensive treatment of these subjects.

A *field* $\mathbb{F}$ is a set of elements with *addition* and *multiplication* operations, and satisfies the following axioms:

(A1) *Closure* under addition and multiplication, that is, for all $a, b \in \mathbb{F}$, both $a + b \in \mathbb{F}$ and $a \cdot b \in \mathbb{F}$;
(A2) *Associativity* of addition and multiplication, that is, for all $a, b, c \in \mathbb{F}$, it holds $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(A3) *Commutativity* of addition and multiplication, that is, for all $a, b \in \mathbb{F}$, it holds $a + b = b + a$ and $a \cdot b = b \cdot a$;
(A4) *Existence of additive and multiplicative identity* elements, that is, for all $a \in \mathbb{F}$, there exist elements $0, 1 \in \mathbb{F}$ such that $a + 0 = a$ and $a \cdot 1 = a$;
(A5) *Existence of additive and multiplicative inverse* elements, that is, for all $a \in \mathbb{F}$, there exist $b, c \in \mathbb{F}$ such that $a + b = 0$ and $a \cdot c = 1$, with $a \neq 0$;
(A6) *Distributivity* of multiplication over addition, that is, for all $a, b, c \in \mathbb{F}$, it holds $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A field is finite if it contains a finite number of elements. A basic class of finite fields are the fields $\mathbb{F}_{\text{p}}$ with characteristic p a prime number. The field $\mathbb{F}_{\text{p}}$ consists of the set of integers $\{0, \dots, p-1\}$, with addition and multiplication defined as in *modular arithmetic*, that is, by performing the operation in the set of integers $\mathbb{Z}$, dividing by p, and taking the remainder.

Let $a : \mathbb{F}_{\mathrm{p}}^m \to \mathbb{F}_{\mathrm{p}}^n$ be a linear map between the vector spaces of dimensions m and n, respectively, over the field $\mathbb{F}_{\mathrm{p}}$. The map a can be represented by a matrix A with n rows and m columns, and elements from the field $\mathbb{F}_{\mathrm{p}}$. The *image* and *kernel* of A are defined as

$$\begin{aligned}\mathrm{Im}(A) &:= \{y \in \mathbb{F}_{\mathrm{p}}^n \ : \ y = Ax, x \in \mathbb{F}_{\mathrm{p}}^m\},\\ \mathrm{Ker}(A) &:= \{x \in \mathbb{F}_{\mathrm{p}}^m \ : \ Ax = 0\},\end{aligned}$$

where additions and multiplications are performed modulo p. Analogously, the *pre-image* of a set of vectors $V \subseteq \mathbb{F}_{\mathrm{p}}^n$ through A is the set

$$A^{-1}(V) := \{x \in \mathbb{F}_{\mathrm{p}}^n \ : \ v = Ax, \text{ for all } v \in V\}.$$

Let $\mathbb{F}_{\mathrm{p}}[s]$ denote the set of polynomials with coefficients in $\mathbb{F}_{\mathrm{p}}$, and let $P_A \in \mathbb{F}_{\mathrm{p}}[s]$ denote the characteristic polynomial of $A \in \mathbb{F}_{\mathrm{p}}^{n\times n}$ over $\mathbb{F}_{\mathrm{p}}$. [1] Let $\sigma_{\mathrm{p}}(A)$ denote the set of eigenvalues of A, that is, the roots of the characteristic polynomial P_A in the field $\mathbb{F}_{\mathrm{p}}$. Notice that the cardinality $|\sigma_{\mathrm{p}}(A)|$ may be strictly smaller than the matrix dimension n, since finite fields are not *algebraically closed*.

We conclude this section with some standard graph definitions. A directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consists of a set of vertices $\mathcal{V}$ and a set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. An edge $(v, w) \in \mathcal{E}$ is directed from vertex w to vertex v. For a vertex $v \in \mathcal{V}$, the set of in-neighbors of v is defined as $\mathcal{N}_v^{\mathrm{in}} = \{w \in \mathcal{V} \ : \ (v, w) \in \mathcal{E}\}$, and the set of out-neighbors as $\mathcal{N}_v^{\mathrm{out}} = \{w \in \mathcal{V} \ : \ (w, v) \in \mathcal{E}\}$. The in-degree of $v \in \mathcal{V}$ equals $|\mathcal{N}_v^{\mathrm{in}}|$, whereas the out-degree of $v \in \mathcal{V}$ equals $|\mathcal{N}_v^{\mathrm{out}}|$. A path in G is a subgraph $P = (\{v_1, \ldots, v_{k+1}\}, \{e_1, \ldots, e_k\})$ such that $v_i \neq v_j$ for all $i \neq j$, and $e_i = (v_{i+1}, v_i)$ for each $i \in \{1, \ldots, k\}$. A cycle is a path in which the first and last vertex in the sequence are the same. The length of a path (resp. cycle) equals the number of edges in the path (resp. cycle). A directed graph is strongly (resp. weakly) connected if there exists a directed (resp. undirected) path between any two vertices. Two subgraphs of the same graph are disjoint if they have no common vertices. A *root* (resp. *globally reachable node*) is a vertex v from which (resp. to which) there exists a directed path to (resp. from) every vertex in the graph, including v itself. Finally, a directed graph is aperiodic if there is no integer greater than one that divides the length of every cycle of the graph.

3 Models of Finite-Field Consensus Networks

Consider a set of $n \in \mathbb{N}_{>0}$ agents, a prime number p, and the finite field $\mathbb{F}_{\mathrm{p}}$. [2] Let the agents interaction be described by the directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $i \in \mathcal{V}$ denotes the i-th agent, with $\mathcal{V} = \{1, \ldots, n\}$, and $(i, j) \in \mathcal{E}$ if there is a directed edge from agent j to agent i. We assume that each agent is able to manipulate and transmit values from the finite field $\mathbb{F}_{\mathrm{p}}$ according to a pre-specified protocol. We focus on distributed protocols in which (i) each agent i is associated with a state $x_i \in \mathbb{F}_{\mathrm{p}}$, and (ii) each agent updates its state as a weighted combination of the states of its in-neighbors $\mathcal{N}_i^{\mathrm{in}}$. Let $a_{ij} \in \mathbb{F}_{\mathrm{p}}$ be the weight associated with the edge (i, j), and let $A = [a_{ij}]$, $A \in \mathbb{F}_{\mathrm{p}}^{n\times n}$, be the *weighted adjacency matrix* of $\mathcal{G}$, or simply *network matrix*, where $a_{ij} = 0$ whenever $(i, j) \notin \mathcal{E}$. Let $x : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\mathrm{p}}^n$ be the vector containing the agents states. The evolution of the network state x over time is described by the iteration (or network)

$$x(t + 1) = Ax(t), \tag{1}$$

where all operations are performed in the field $\mathbb{F}_{\mathrm{p}}$.

The *transition graph* associated with the iteration (1) over $\mathbb{F}_{\mathrm{p}}$ is defined as $\mathcal{G}_A = (\mathcal{V}_A, \mathcal{E}_A)$, where, $\mathcal{V}_A = \{v \ : \ v \in \mathbb{F}_{\mathrm{p}}^n\}$ and, for $v_i, v_j \in \mathcal{V}_A$, the edge $(v_i, v_j) \in \mathcal{E}_A$ if and only if $v_i = Av_j$. It should be observed that the transition graph contains p^n vertices, and that each vertex has unit out-degree. Moreover, it can be shown that the transition graph is composed of disjoint weakly-connected subgraphs, and that each subgraph contains exactly one cycle, possibly of unit length [20]. Finally, each disjoint subgraph contains a globally reachable node. This particular structure of the transition graph will be used to derive certain results on finite-field consensus. Examples of transition graphs are given below in Fig. 1 and Fig. 2.

Consensus networks with real-valued weights and states have been extensively studied [2, 10]. In this work we show that real-valued consensus networks and finite-field consensus networks exhibit different features, and particular care needs to be taken to ensure the desired properties over finite fields. For instance, consensus networks over the field of real numbers usually converge asymptotically, [3] while finite-field consensus networks can only achieve consensus in a finite number of iterations, since the state space contains a finite number of states. Thus we say that the iteration (1) (or simply the network matrix A) over a finite field **achieves consensus**, if for all initial states $x(0) \in \mathbb{F}_{\mathrm{p}}^n$ there exists a finite time $T \in \mathbb{N}$ such that $x(T) = x(T + \tau) = \alpha\mathbb{1}$ for all $\tau \in \mathbb{N}$, $\mathbb{1} = [1 \ \ldots \ 1]^{\mathsf{T}}$, and for some $\alpha \in \mathbb{F}_{\mathrm{p}}$. We conclude this section with a simple result. A matrix A over the field $\mathbb{F}_{\mathrm{p}}$ is *nilpotent* if $A^n = 0$ and is *row-stochastic* if $A\mathbb{1} = \mathbb{1}$.

[1] Since the characteristic polynomial $\bar{P}_A(s) \in \mathbb{R}[s]$ has only integer coefficients for any $A \in \mathbb{F}_{\mathrm{p}}^{n\times n}$, the characteristic polynomial $P_A(s) \in \mathbb{F}_{\mathrm{p}}[s]$ is $\sum_{i=0}^n \mathrm{mod}(\bar{c}_i, p)s^i$, where $\mathrm{mod}(\cdot)$ is the modulus function, and $\bar{c}_i$ is the i-th coefficient of $\bar{P}_A(s)$.

[2] Our results rely on properties of the vector space $\mathbb{F}_{\mathrm{p}}^n$. Hence, p must be a prime number or a power of a prime number [18]. Without affecting generality, we only consider the case where p is a prime number.

[3] De Bruijn networks are an exception, as they converge in finite-time over the field of real numbers [21]. However, de Bruijn networks have specific structure, while finite-field consensus networks include a broader class of graph structures.

Lemma 3.1 ***(Finite-field consensus matrices)*** *Consider the iteration* (1) *over the field* $\mathbb{F}_{\mathrm{p}}$*. If consensus is achieved, then* A *is either nilpotent or row-stochastic.* [4]

A proof of Lemma 3.1 is omitted in the interest of space. As for the case of real-valued consensus, we limit our attention to row-stochastic network matrices. Although consensus is achieved whenever the network matrix is nilpotent, this case is of limited interest because the consensus value is independent of the agents initial states.

4 Analysis of Finite-Field Consensus Networks

Conditions for consensus in real-valued networks have been deeply investigated in the last years [2, 10]. For instance, sufficient conditions ensuring real-valued consensus are that the network matrix A is row-stochastic and that the associated directed graph is strongly connected and aperiodic. The following example shows that graph-theoretic properties are not sufficient for an iteration over a finite field to achieve consensus.

Example 1 ***(Graph properties are not sufficient for finite-field consensus)*** *Consider a fully connected network with three agents over the field* $\mathbb{F}_3$*. Consider the network matrices* $A_1 = \begin{bmatrix} 2 & 1 & 1 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix}$, $A_2 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 1 \end{bmatrix}$*, and* $A_3 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$*. Notice that* A_1*,* A_2*, and* A_3 *are row-stochastic and their interaction graph is fully connected. It can be verified that over the field* $\mathbb{F}_3$ *only the network matrix* A_1 *achieves consensus, while* A_2 *and* A_3 *exhibit oscillatory dynamics for certain initial conditions. An example of oscillatory dynamics generated by the network matrix* A_3 *is reported in Table 1.*

Table 1
Sample state trajectory for the matrix A_3 in Example 1.

$x(0)$	$x(1)$	$x(2)$	$x(3)$	$x(4)$	$x(5)$	$x(6)$
1	2	0	1	2	0	1
0	1	2	0	1	2	0
0	1	2	0	1	2	0

Since the considered network matrices feature the same connectivity properties and yet only one of them achieves finite-field consensus, we conclude that graph properties are not sufficient to guarantee finite-field consensus. □

The dynamics of an iteration over a finite field is entirely described by its associated transition graph. The next theorem provides a necessary and sufficient condition for finite-field consensus based on the transition graph.

Theorem 4.1 ***(Transition graph of a consensus network)*** *Consider the iteration* (1) *over the field* $\mathbb{F}_{\mathrm{p}}$ *with row-stochastic matrix* A*, and let* $\mathcal{G}_A = (\mathcal{V}_A, \mathcal{E}_A)$ *be its associated transition graph. The following statements are equivalent:*

(i) the iteration (1) *achieves consensus, and*
(ii) the transition graph $\mathcal{G}_A$ *contains exactly* p *cycles, corresponding to the unit cycles around the vertices* $\alpha\mathbb{1}$ *for* $\alpha \in \{0, \dots, p-1\}$*.*

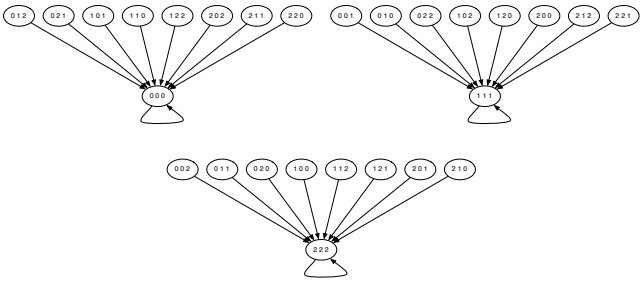

Fig. 1. Transition graph $\mathcal{G}_{A_1}$ associated with the matrix $A_1 \in \mathbb{F}_3^{3\times 3}$ in Example 1. Since $\mathcal{G}_{A_1}$ contains exactly 3 cycles corresponding to the self-loops around the consensus vertices, the matrix A_1 achieves consensus; see Theorem 4.1.

PROOF. *(i)* $\implies$ *(ii)* Since the iteration achieves consensus, it follows from Lemma 3.1 that $A\mathbb{1} = \mathbb{1}$. Hence, the transition graph contains p unit cycles corresponding to the vertices $\alpha\mathbb{1} \in \mathcal{V}_A$, with $\alpha \in \mathbb{F}_{\mathrm{p}}$. Suppose by contradiction that there exists an additional cycle C, and notice that the vertices $\alpha\mathbb{1}$, with $\alpha \in \mathbb{F}_{\mathrm{p}}$, cannot be contained in C since the out-degree of each vertex in the transition graph is exactly one (the transition graph is determined by the linear map A). Thus, there exists a trajectory along C that does not converge to consensus, which contradicts the initial hypothesis.

(ii) $\implies$ *(i)* Notice that a state trajectory of the iteration (1) is in bijective correspondence with a path on the transition graph $\mathcal{G}_A$. Suppose that transition graph $\mathcal{G}_A$ contains exactly p unit cycles located at the vertices $\alpha\mathbb{1} \in \mathcal{V}_A$, with $\alpha \in \mathbb{F}_{\mathrm{p}}$. Then, since each vertex in the transition graph has unit out-degree, every (sufficiently long) path in $\mathcal{G}_A$ eventually reaches one of the cycles and, consequently, every state trajectory converges to a consensus state. □

Example 2 ***(Transition graph of a consensus network)*** *The transition graphs associated with the matrices* A_1 *and* A_3 *in Example 1 over the field* $\mathbb{F}_3$ *are reported in Fig. 1 and Fig. 2, respectively. As previously discussed, and as predicted by Theorem 4.1, the matrix* A_1 *achieves consensus, while the matrix* A_3 *does not.* □

Theorem 4.1 provides a necessary and sufficient condition for finite-field consensus based on the transition graph. From condition (ii) in Theorem 4.1 and the fact that each vertex in the transition graph has unit out-degree, the transition graph of a consensus matrix is

[4] This result is general, and it also applies to iterations over the field of real numbers.

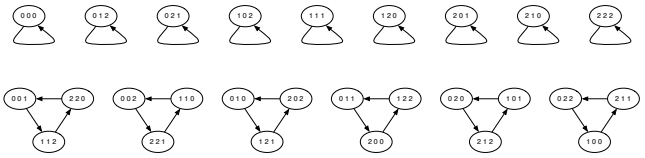

Fig. 2. Transition graph $\mathcal{G}_{A_3}$ associated with the matrix $A_3 \in \mathbb{F}_3^{3\times 3}$ in Example 1. Since $\mathcal{G}_{A_3}$ contains more than 3 cycles, the matrix A_3 does not achieve consensus; see Theorem 4.1. The oscillatory state trajectory in Table 1 corresponds to the bottom right cycle in this figure.

composed of p disjoint weakly-connected subgraphs, all with the same graph topology [20, Proposition 3.4].

A verification of the convergence condition in Theorem 4.1 may be prohibitive for large networks, because the size of the transition graph grows exponentially with the number of agents in the network (the transition graph contains p^n vertices and p^n edges, since each vertex has unit out-degree). In what follows we shall derive consensus conditions based on the network matrix instead of its transition graph. Consider the *inverse recursion*

$$\mathcal{S}_\alpha^{t+1} = A^{-1}(\mathcal{S}_\alpha^t), \tag{2}$$

where $\mathcal{S}_\alpha^t \subset \mathbb{F}_{\rm p}^n$ for all times t and $\mathcal{S}_\alpha^0 = \{\alpha\mathbb{1}\}$. Notice that the inverse recursion defines a sequence of sets, and that the set $\mathcal{S}_\alpha^t$ contains the initial states converging to the consensus value $\alpha\mathbb{1}$ in at most t iterations. We say that the recursion (2) is convergent with limiting set $\mathcal{S}_\alpha$ if there exists $T < n$ satisfying $\mathcal{S}_\alpha = \mathcal{S}_\alpha^T = \mathcal{S}_\alpha^{T+1}$.

Theorem 4.2 ***(Recursion subspaces of a consensus network)*** *Consider the iteration* (1) *over the field* $\mathbb{F}_{\rm p}$ *with row-stochastic matrix* A*. The following statements are equivalent:*

(i) the iteration (1) *achieves consensus,*
(ii) there exists $\alpha \in \mathbb{F}_{\rm p}$ *such that the recursion* (2) *is convergent and the limiting set* S_α *satisfies* $|\mathcal{S}_\alpha| = p^{n-1}$*, and*
(iii) for all $\alpha \in \mathbb{F}_{\rm p}$ *the recursion* (2) *is convergent and each limiting set* S_α *satisfies* $|\mathcal{S}_\alpha| = p^{n-1}$*.*

PROOF. Consider the transition graph $\mathcal{G}_A = (\mathcal{V}, \mathcal{E})$, and define the reverse graph $\bar{\mathcal{G}}_A = (\mathcal{V}, \bar{\mathcal{E}})$, where $(i,j) \in \bar{\mathcal{E}}$ if and only if $(j,i) \in \mathcal{E}$. Notice that the recursion (2) is convergent if and only if $\bar{\mathcal{G}}_A$ contains no cycle of length greater than 1 reachable from $\alpha\mathbb{1}$. Recall from [20, Theorem 1] that $\mathcal{G}_A$ (resp. $\bar{\mathcal{G}}_A$) is obtained as the graph product of a tree by a set of cycles. Hence, the graph $\mathcal{G}_A$ (resp. $\bar{\mathcal{G}}_A$) is composed of disjoint weakly-connected subgraphs, and disjoint subgraphs have the same structure. From this argument we conclude that (ii) and (iii) are equivalent.

(i) $\implies$ *(ii)* Since A achieves consensus, the graph $\mathcal{G}_A$ contains exactly p unit cycles corresponding to the consensus vertices (see Theorem 4.1 and Fig. 1). By [20, Theorem 1], the above reasoning, and the fact that A achieves consensus, it follows that $|\mathcal{S}_0| + \cdots + |\mathcal{S}_{p-1}| = p^n$, and that $|\mathcal{S}_\alpha| = p^{n-1}$ for all $\alpha \in \mathbb{F}_{\rm p}$.

(ii) $\implies$ *(i)* Since $A\mathbb{1} = \mathbb{1}$, the transition graph contains p cycles of unit length located at the consensus vertices. Let the recursion (2) be convergent for some $\alpha \in \mathbb{F}_{\rm p}$. From [20, Theorem 1], the graph $\mathcal{G}_A$ contains p identical, disjoint, weakly-connected subgraphs, each one terminating in a consensus vertex. Since $|\mathcal{S}_\alpha| = p^{n-1}$, it follows that consensus is achieved from p^n states (every initial state), which concludes the proof. □

Example 3 ***(Inverse recursion for a finite-field consensus network)*** *For the matrix* $A_1 \in \mathbb{F}_3^{3\times 3}$ *in Example 1, the set* $\mathcal{S}_1$ *generated by* (2) *is*

$$\mathcal{S}_1 = \left\{ \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\2\\2\end{bmatrix}, \begin{bmatrix}1\\0\\2\end{bmatrix}, \begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}2\\1\\2\end{bmatrix}, \begin{bmatrix}2\\2\\1\end{bmatrix} \right\}.$$

Because $|\mathcal{S}_1| = 3^2$*, the network matrix* A_1 *achieves consensus due to Theorem 4.2. Instead, for the network matrix* $A_3 \in \mathbb{F}_3^{3\times 3}$ *in Example 1, the inverse recursion yields* $\mathcal{S}_1 = \{\mathbb{1}\}$*, so that* A_3 *does not achieve consensus.* □

According to Theorem 4.2, the convergence of the network (1) can be determined by iterating the inverse recursion (2) for some $\alpha \in \mathbb{F}_{\rm p}$. This computation does not require analyzing the transition graph. Our last and most explicit condition for finite-field consensus is based upon the characteristic polynomial of the network matrix (computed over the finite field).

Theorem 4.3 ***(Characteristic polynomial of a consensus network)*** *Consider the iteration* (1) *over the finite field* $\mathbb{F}_{\rm p}$ *with row-stochastic matrix* A*. The following statements are equivalent:*

(i) the iteration (1) *achieves consensus, and*
(ii) $P_A(s) = s^{n-1}(s-1)$*.*

Example 4 ***(Characteristic polynomial of consensus matrices)*** *Consider the network matrices in Example 1 over the field* $\mathbb{F}_3$*. It can be verified that*

$$P_{A_1}(s) = s^2(s-1), \;\; P_{A_2}(s) = s(s^2-2s+1), \;\; \textit{and}$$
$$P_{A_3}(s) = s^3 - 1.$$

As predicted by our previous analysis and by Theorem 4.3, only the network matrix A_1 *achieves consensus.* □

The proof of this Theorem 4.3 is postponed to the Appendix. Theorem 4.3 is equivalently restated as follows: A achieves finite-field consensus if and only if $\sigma_{\rm p}(A) = \{1, 0, \ldots, 0\}$. In other words, the characteristic polynomial of a finite-field matrix achieving consensus

can be factored into polynomials of unit degree over the field and, consequently, every finite-field matrix achieving consensus can be represented in Jordan canonical form via a similarity transformation; see [22] and [23, Theorem 3.5]. We finally characterize the convergence value of a consensus network over a finite field.

Theorem 4.4 ***(Finite-field consensus time and value)*** *Consider the iteration* (1) *over the finite field* $\mathbb{F}_{\mathrm{p}}$ *with row-stochastic matrix* A *and with initial state* $x(0) \in \mathbb{F}_{\mathrm{p}}^n$. *Assume the iteration* (1) *achieves consensus. Let* $T < n$ *denote the dimension of the largest Jordan block associated with the eigenvalue* 0. *Let* $\pi \in \mathbb{F}_{\mathrm{p}}^n$ *be the unique eigenvector satisfying* $\pi A = \pi$ *and* $\pi \mathbb{1} = 1$. *Then* $A^T = \mathbb{1}\pi$, *so that consensus is achieved at the value* $\pi x(0)$ *after* T *iterations. Moreover, the* i*-th component of* π *is nonzero only if the* i*-th vertex of the directed graph associated with* A *is a root.*

PROOF: Since A achieves consensus, we have $\sigma_{\mathrm{p}}(A) = \{1, 0, \ldots, 0\}$, and A admits a Jordan canonical form $J_A = V^{-1}AV$ over $\mathbb{F}_{\mathrm{p}}$. Moreover, the matrix A converges in $T < n$ iterations. The next part of the proof follows the reasoning in [24, Theorem 3]. Let the first column of V be $\mathbb{1}$, and notice that the first row of the matrix J_A has only zero elements, except for the first entry which has unit value. Since $V^{-1}A = J_A V^{-1}$, the first row of V^{-1}, say π, satisfies $\pi A = \pi$. Then $A^T = V J_A^T V^{-1} = \mathbb{1}\pi$. Since $A\mathbb{1} = \mathbb{1}$, it follows that $\mathbb{1} = A^T\mathbb{1} = \mathbb{1}\pi\mathbb{1}$, and consequently $\pi\mathbb{1} = 1$. To show the last statement, let $\mathcal{G}$ be the directed graph associated with A, and let i be a vertex of $\mathcal{G}$. Assume that i is not a root of $\mathcal{G}$, and let the initial state $x(0)$ be all zeros, except for the i-th component. Since i is not a root, there exists a node j which is not reachable from i, and, consequently, the value of the j-th agent is not affected by the i-th agent. Since A achieves consensus for all initial states, the j-th entry of $\mathbb{1}\pi x(0)$ needs to be zero, from which the statement follows. □

Observe that Theorem 4.4 is not a direct consequence of the theory of non-negative matrices over the field of real numbers [22]. In fact, if regarded as a real-valued matrix, a finite-field consensus matrix is generally unstable.

5 Design of Finite-Field Consensus Networks

In Section 4 we characterize the convergence of consensus networks over finite fields. With respect to consensus networks over the field of real numbers, finite-field consensus networks require less computational effort and communication bandwidth, and they converge in a finite number of iterations. On the other hand, convergence conditions for finite-field consensus networks depend on the numerical entries of the network matrix (Theorem 4.3), and not only on the connectivity properties of the underlying graph as in the case of consensus networks with real values. For this reason, the design of finite-field consensus networks deserves particular attention. In this section we describe methods to design finite-field consensus networks, and we discuss their limitations.

5.1 Network design via characteristic polynomial

The objective of this section is to design a finite-field consensus matrix A whose sparsity patter is compatible with a given agents interaction graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, that is, to design a network matrix $A = [a_{ij}]$, $a_{ij} \in \mathbb{F}_{\mathrm{p}}$, where p is a given prime number, and $a_{ij} \neq 0$ only if (i, j) is an edge of $\mathcal{G}$. Recall from Theorem 4.3 that the network matrix A achieves consensus if and only if its characteristic polynomial is $P_A(s) = s^{n-1}(s-1)$ and $A\mathbb{1} = \mathbb{1}$. Since two polynomials are equal if and only if all coefficients are equal, the entries of A can be determined by simultaneously solving the following equations:

$$\begin{cases} A \in \mathbb{F}_{\mathrm{p}}^{n\times n}, \text{ with } a_{ij} = 0 \text{ if } (i,j) \notin \mathcal{E}, \\ \mathbb{1} = A\mathbb{1}, \\ 1 = -c(A, n-1), \\ 0 = c(A, j), \quad j \in \{0, \ldots, n-2\}, \end{cases} \tag{3}$$

where $c(A, d)$ is the coefficient of the monomial of degree d in the (parametric) characteristic polynomial P_A.

Notice that the system of equations (3) contains nonlinear, multivariate, polynomial equations, where the unknown variables are the entries of the network matrix A, and that a solution is required over the finite field $\mathbb{F}_{\mathrm{p}}$. The problem of solving systems of multivariate polynomial equations over finite fields is *NP-hard* [25], and it is one of the important research problems in cryptography and information security [26]. Besides enumerating all possible solution candidates, [5] several solution techniques have been proposed over the last years, see for instance [27, 28]. We next provide a condition for the existence of finite-field consensus networks.

Theorem 5.1 ***(Existence of finite-field consensus matrices)*** *Let* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ *be the directed agents interaction graph, with* $|\mathcal{V}| = n$ *and* $|\mathcal{E}| = m$. *Assume that* $\mathcal{G}$ *contains a root, and that* $m > \frac{n^2+n}{2}$. *Then the system of equations* (3) *admits* $N \geq p^{\frac{2m-n^2-n}{2}}$ *solutions over the field* $\mathbb{F}_{\mathrm{p}}$, *where* N *is divisible by the characteristic* p. *In other words, there exist* N *network matrices* $A = [a_{ij}]$ *achieving consensus, with* $a_{ij} \in \mathbb{F}_{\mathrm{p}}^{n\times n}$ *and* $a_{ij} = 0$ *if* $(i, j) \notin \mathcal{E}$.

PROOF: Let $c(A, d)$ be the coefficient of the monomial of degree d in the parametric characteristic polynomial P_A, with $A = [a_{ij}]$ and $a_{ij} = 0$ if $(i, j) \notin \mathcal{E}$.

[5] If m is the number of free entries in A, a brute-force solution to (3) requires computing all p^m possible matrices A compatible with the interaction graph $\mathcal{G}$.

Define the polynomial $f_i \in \mathbb{F}_{\rm p}[a_{ij}]$ with $(i,j) \in \mathcal{E}$ as: $f_i = f_i(a_{ij}) = \sum_{j=1}^{n} a_{ij} - 1$ for $i \in \{1,\dots,n\}$, $f_{n+1} = 1 + c(A, n-1)$, and $f_i = c(A, 2n-i)$ for $i \in \{n+2,\dots,2n\}$. Notice that a solution to (3), and hence a finite-field consensus matrix compatible with $\mathcal{G}$, can be computed by simultaneously solving the equations $f_i = 0$ for $i \in \{1,\dots,2n\}$. Observe that $\deg(f_i) = 1$ for $i \in \{1,\dots,n\}$, and $\deg(f_i) \leq i - n$ for $i \in \{n+1,\dots,2n\}$. Then $\sum_{i=1}^{2n} \deg(f_i) \leq n + \frac{n(n-1)}{2} \leq \frac{n^2+n}{2}$. Since $m > \frac{n^2+n}{2}$ by assumption, we conclude from [6, Theorem 6.8] that the number of simultaneous solutions N to the equations $f_i = 0$, $i \in \{1,\dots,2n\}$, in the field $\mathbb{F}_{\rm p}$ is divisible by the characteristic p. To show that $N \geq p^{\frac{2m-n^2-n}{2}}$, we next construct a network matrix A achieving consensus and compatible with the interaction graph $\mathcal{G}$ (in fact our construction only requires the existence of a root in $\mathcal{G}$), and then employ [6, Theorem 6.11]. Let v be a root of $\mathcal{G}$, and let $S = (\mathcal{V}, \mathcal{E}_S)$ be a rooted spanning tree of $\mathcal{G}$ with root v, and with $(v,v) \in \mathcal{E}_S$ and $(i,i) \notin \mathcal{E}_S$ for $i \neq v$. Relabel the vertices $\mathcal{V}$ according to their distance from the root v. Define the matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if $(i,j) \in \mathcal{E}_S$, and $a_{ij} = 0$ otherwise. Notice that $A \in \mathbb{F}_{\rm p}^{n\times n}$ is triangular and row-stochastic, and that its diagonal elements are $\{1,0,\dots,0\}$. It follows from Theorem 4.3 that A achieves consensus. □

In view of Theorem (5.1), consensus over finite fields is possible on a broad class of interaction graphs. A complete characterization of all the interaction topologies yielding consensus over finite fields is beyond the scope of this work, and it is left as the subject of future research. We conclude this section with a remark.

Remark 1 ***(Network design for fully connected graphs)*** *Let the agents interaction graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be fully connected, that is $(i,j) \in \mathcal{E}$ for all $i,j \in \{1,\dots,n\}$. Let $v \in \mathbb{F}_{\rm p}^{1\times n}$ be any vector satisfying $v\mathbb{1} = 1$. Then the network matrix $A = [v^{\mathsf{T}} \cdots v^{\mathsf{T}}]^{\mathsf{T}}$ achieves consensus over $\mathbb{F}_{\rm p}$; see for instance the matrix A_1 in Example 1. To see this, let $\mathbb{1}_{\rm orth} \in \mathbb{F}_{\rm p}^{n\times(n-1)}$ be any full column rank matrix satisfying $v\mathbb{1}_{\rm orth} = 0$. Since $A\mathbb{1} = \mathbb{1}$, and $A\mathbb{1}_{\rm orth} = 0$, we have $\sigma_{\rm p}(A) = \{1,0,\dots,0\}$, $|\sigma_{\rm p}(A)| = n$, and the claimed statement follows from Theorem 4.3.* □

5.2 Network design via network composition

In this section we use the concept of graph products to generate finite-field consensus networks from smaller consensus components. Let $A \otimes B$ denote the *Kronecker product* of the matrices A and B over the field $\mathbb{F}_{\rm p}$ [22].

Theorem 5.2 ***(Finite-field consensus via Kronecker product)*** *Consider the network matrices $A \in \mathbb{F}_{\rm p}^{n\times n}$ and $B \in \mathbb{F}_{\rm p}^{m\times m}$, and assume that A and B achieve consensus. Then the network matrix $A \otimes B \in \mathbb{F}_{\rm p}^{nm\times nm}$ achieves consensus.*

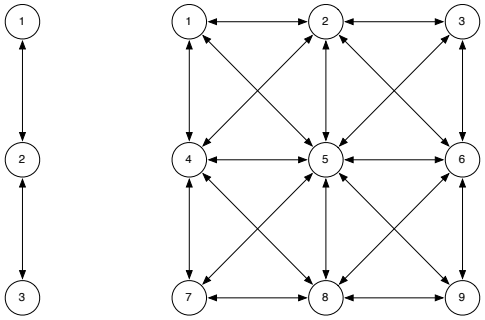

Fig. 3. Agents interaction graphs (without self-loops) for the matrices A (left) and $A_{\rm k} = A \otimes A$ (right) in Example 5.

PROOF. We first show that $(A \otimes B)$ is row-stochastic. Let $\mathbb{1}_n$ be the vector of all ones of dimension n. Since A and B are row-stochastic over $\mathbb{F}_{\rm p}$, we have

$$(A\otimes B)\mathbb{1}_{nm} = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix} \mathbb{1}_{nm}$$
$$= \begin{bmatrix} \sum_{j=1}^{n} a_{1,j}B\mathbb{1}_m \\ \sum_{j=1}^{n} a_{2,j}B\mathbb{1}_m \\ \vdots \\ \sum_{j=1}^{n} a_{n,j}B\mathbb{1}_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{n} a_{1,j}\mathbb{1}_m \\ \sum_{j=1}^{n} a_{2,j}\mathbb{1}_m \\ \vdots \\ \sum_{j=1}^{n} a_{n,j}\mathbb{1}_m \end{bmatrix} = \mathbb{1}_{nm}.$$

Let $J_A = P^{-1}AP$ and $J_B = Q^{-1}BQ$ be the canonical Jordan form of A and B, respectively [23, Theorem 3.5]. Then $J_A \otimes J_B = (P^{-1}AP) \otimes (Q^{-1}BQ) = (P^{-1} \otimes Q^{-1})(A\otimes B)(P\otimes Q) = (P\otimes Q)^{-1}(A\otimes B)(P\otimes Q)$, so that $A \otimes B$ and $J_A \otimes J_B$ are similar. Thus the eigenvalues of $A\otimes B$ are the same as those of $J_A \otimes J_B$, and, because J_A and J_B are upper triangular with eigenvalues λ_i and μ_i on the diagonal, we conclude that $J_A \otimes J_B$ is also upper triangular with diagonal entries, and eigenvalues, $\lambda_i\mu_j$. Since $\sigma_{\rm p}(A) = \{1,0,\dots,0\}$ and $\sigma_{\rm p}(B) = \{1,0,\dots,0\}$, the statement follows from Theorem 4.3. □

Example 5 ***(Finite-field consensus network via Kronecker product)*** *Consider the network matrix $A = \left[\begin{smallmatrix} 9 & 3 & 0 \\ 1 & 9 & 2 \\ 0 & 7 & 5 \end{smallmatrix}\right]$ over the field $\mathbb{F}_{11}$. It can be verified that A achieves consensus. By Theorem 5.2 the network matrix*

$$A_{\rm k} = A \otimes A = \begin{bmatrix} 4 & 5 & 0 & 5 & 9 & 0 & 0 & 0 & 0 \\ 9 & 4 & 7 & 3 & 5 & 6 & 0 & 0 & 0 \\ 0 & 8 & 1 & 0 & 10 & 4 & 0 & 0 & 0 \\ 9 & 3 & 0 & 4 & 5 & 0 & 7 & 6 & 0 \\ 1 & 9 & 2 & 9 & 4 & 7 & 2 & 7 & 4 \\ 0 & 7 & 5 & 0 & 8 & 1 & 0 & 3 & 10 \\ 0 & 0 & 0 & 8 & 10 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 7 & 8 & 3 & 5 & 1 & 10 \\ 0 & 0 & 0 & 0 & 5 & 2 & 0 & 2 & 3 \end{bmatrix}$$

achieves consensus over $\mathbb{F}_{11}$. In fact, it can be verified that $P_{A_{\rm k}} = s^8(s-1)$ and $A_{\rm k}\mathbb{1} = \mathbb{1}$. Moreover, the network

matrices A and A_{k} have the same convergence speed. The interaction graph of A and A_{k} are reported in Fig. 3. □

Following Theorem 5.2, finite-field consensus networks can be constructed by composing smaller components. We refer the interested reader to [29] for a comprehensive discussion of graphs generated via Kronecker product of adjacency matrices. Regarding the convergence speed of finite-field consensus networks generated via Kronecker products, the following holds. Let $A_{\mathrm{k}} = A_1 \otimes \cdots \otimes A_m$, and let s_i be the number of iterations needed for convergence of the networks A_i, $i \in \{1, \ldots, m\}$. Due to [22, Theorem 4.3.17], the network A_{k} converges exactly in $\max\{s_1, \ldots, s_m\}$ iterations. In other words, the consensus network A_{k} is as fast as the slowest of its components.

6 Application to Average Consensus and Distributed Pose Estimation

In this section we present applications of finite-field consensus, namely average consensus and pose estimation.

6.1 Finite-time average consensus

Given a sensor network, let $x_0 \in \mathbb{F}_{\mathrm{p}}^n$ be the vector containing the agents initial states. Let $x_{\mathbb{R}} = \mathbb{1}^{\mathsf{T}} x_0 / n \in \mathbb{R}$ be the average of the agents initial states over the field of real numbers. The average of the agents initial states over the field $\mathbb{F}_{\mathrm{p}}$ can be computed by means of Fermat's Little Theorem [30] as $x_{\mathbb{F}} = n^{p-2} \mathbb{1}^{\mathsf{T}} x_0 \in F_{\mathrm{p}}$, where we assume $n \neq kp$ for all $k \in \mathbb{N}$, for the inverse of n over $\mathbb{F}_{\mathrm{p}}$ to exist. In what follows, first we show how to compute the average $x_{\mathbb{F}}$ by means of finite-field consensus networks. Then we describe conditions that allow to recover the average $x_{\mathbb{R}}$ from the knowledge of $x_{\mathbb{F}}$ and the total number of agents.

We say that the iteration (1) over the field $\mathbb{F}_{\mathrm{p}}$ achieves average consensus if it achieves consensus, and the consensus value is $n^{p-2} \mathbb{1}^{\mathsf{T}} x_0$ for every initial state x_0.

Theorem 6.1 ***(Finite-field average consensus)*** *Consider the iteration* (1) *over the field $\mathbb{F}_{\mathrm{p}}$ with row-stochastic matrix A. Assume that the field characteristic satisfies $n \neq kp$ for all $k \in \mathbb{N}$. The following statements are equivalent:*

(i) the iteration (1) *achieves average consensus, and*
(ii) $P_A(s) = s^{n-1}(s-1)$, and $\mathbb{1}^{\mathsf{T}} A = \mathbb{1}^{\mathsf{T}}$.

PROOF of Theorem 6.1: *(i)* $\implies$ *(ii)* Since the iteration achieves consensus, it follows from Theorem 4.4 that $A^n = \mathbb{1}\pi$, where π satisfies $\pi A = \pi$. Because A achieves average consensus, it needs to be $\mathbb{1}\pi = n^{p-2}\mathbb{1}\mathbb{1}^{\mathsf{T}}$. Then $\pi = n^{p-2}\mathbb{1}^{\mathsf{T}}$, and $\mathbb{1}^{\mathsf{T}} A = \mathbb{1}^{\mathsf{T}}$.

Fig. 4. A subgraph of the transition graph associated with the network matrix A in Example 6. Since the sum of the initial states is maintained, average consensus is achieved.

(ii) $\implies$ *(i)* Since $P_A(s) = s^{n-1}(s-1)$ and $A\mathbb{1} = \mathbb{1}$, it follows from Theorem 4.3 that the network achieves consensus. Notice that $\mathbb{1}^{\mathsf{T}} A = \mathbb{1}^{\mathsf{T}}$ implies that $\mathbb{1}^{\mathsf{T}} x(t) = \mathbb{1}^{\mathsf{T}} x(0)$ at all times time t. Let α be the consensus value, and notice that $n\alpha = \mathbb{1}^{\mathsf{T}} x(0)$. To conclude the proof, $\alpha = n^{p-2}\mathbb{1}^{\mathsf{T}} x(0)$, and the network achieves average consensus. □

Example 6 ***(An example of finite-field average consensus)*** *Consider the network matrix $A = \begin{bmatrix} 2 & 3 & 1 \\ 2 & 4 & 0 \\ 2 & 4 & 0 \end{bmatrix}$ over the field $\mathbb{F}_5$. It can be verified that $A\mathbb{1} = \mathbb{1}$, $\mathbb{1}^{\mathsf{T}} A = \mathbb{1}^{\mathsf{T}}$, and $P_A = s^2(s-1)$. By Theorem 6.1 the network matrix A achieves average consensus over $\mathbb{F}_5$. In Fig. 4 we show a subgraph of the transition graph associated with A.* □

Theorem 6.1 provides a necessary and sufficient condition for a network with $n \neq kp$ agents to achieve average consensus over $\mathbb{F}_{\mathrm{p}}$. The condition $n \neq kp$ is actually necessary for average consensus. In other words, if $n = kp$ for some $k \in \mathbb{N}$, then there exists no network matrix satisfying all conditions in Theorem 6.1 and, therefore, average consensus cannot be achieved. To see this, let $x(0)$ be the network initial state, with $\mathbb{1}^{\mathsf{T}} x(0) \neq 0$, and assume by contradiction that α is the corresponding consensus value. Since $\mathbb{1}^{\mathsf{T}} x(t) = \mathbb{1}^{\mathsf{T}} x(0)$ at all times t, it needs to be $n\alpha = \mathbb{1}^{\mathsf{T}} x(0)$. Then $0 = n\alpha = \mathbb{1}^{\mathsf{T}} x(0) \neq 0$, since kp and 0 are in fact the same element in $\mathbb{F}_{\mathrm{p}}$.

Suppose now that the average $x_{\mathbb{F}}$ has been computed, and that each agent knows the total number of agents, the field characteristic, and its own initial state. With these assumptions, it is generally not possible to recover the average $x_{\mathbb{R}}$. To see this, consider the case $n = 3$, $p = 5$, and the initial conditions $x_1 = [2\ 2\ 2]^{\mathsf{T}}$ and $x_2 = [0\ 0\ 1]^{\mathsf{T}}$. Over the field of real numbers we have $x_{1,\mathbb{R}} = \mathbb{1}^{\mathsf{T}} x_1 / n = 2$ and $x_{2,\mathbb{R}} = \mathbb{1}^{\mathsf{T}} x_2 / n = 1/3$. Over the field $\mathbb{F}_{\mathrm{p}}$, instead, $x_{1,\mathbb{F}} = n^{p-2}\mathbb{1}^{\mathsf{T}} x_1 = 2$ and $x_{2,\mathbb{F}} = n^{p-2}\mathbb{1}^{\mathsf{T}} x_2 = 2$. Since $x_{1,\mathbb{F}} = x_{2,\mathbb{F}}$ and $x_{1,\mathbb{R}} \neq x_{2,\mathbb{R}}$, it is not possible to recover the average value over the field of real numbers from the average over a finite field and knowledge of network cardinality and parameters.

Theorem 6.2 ***(Average computation)*** *Let $x_0 \in \mathbb{F}_{\mathrm{p}}^n$, let $x_{\mathbb{R}} = \mathbb{1}^{\mathsf{T}} x_0 / n \in \mathbb{R}$, and let $x_{\mathbb{F}} = n^{p-2}\mathbb{1}^{\mathsf{T}} x_0$, with $n \neq kp$ for all $k \in \mathbb{N}$. If the field characteristic satisfies $n\|x_0\|_\infty \leq p$, then $x_{\mathbb{R}} = mod(n\, x_{\mathbb{F}}, p)/n$.*

PROOF: The statement follows from the relation $\mathrm{mod}(n\, x_{\mathbb{F}}, p) = \mathrm{mod}(n^{p-1}\mathbb{1}^{\mathsf{T}} x_0, p) = \mathbb{1}^{\mathsf{T}} x_0$, where the last equality holds because $\mathrm{mod}(n^{p-1}, p) = 1$, and $n\|x_0\|_\infty \leq p$. □

We conclude this part by noticing that the condition $n\|x_0\|_\infty \leq p$ in Theorem 6.2 is not restrictive. In fact, the field characteristic p is a design parameter and, in general, it can be chosen to satisfy the above condition as long as the network cardinality n and a bound on the agents initial state are known.

6.2 Pose estimation from relative measurements

In this section we use our previous analysis to calibrate the orientation of a network of cameras. This problem has been previously considered in [31] as a distributed estimation problem over $SO(2)$. With respect to the existing literature, we let the measurements and the orientations take value in a pre-specified finite field, and we develop an estimation algorithm with performance guarantees based on modular arithmetic.

A camera network is modeled by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where each vertex is associated with a camera. Let $n = |\mathcal{V}|$ and $m = |\mathcal{E}|$. Let $\theta_i : \mathbb{N}_{\geq 0} \to \mathcal{O}_p$ be the orientation of the i-th camera as a function of time where, for some prime number p,

$$\mathcal{O}_p := \left\{ k\frac{2\pi}{p} : k \in \{0, \dots, p-1\} \right\}. \tag{4}$$

We refer to p as to *discretization accuracy*. For notational convenience, we define the directed graph $\mathcal{G}_{\mathrm{d}} = (\mathcal{V}_{\mathrm{d}}, \mathcal{E}_{\mathrm{d}})$ associated with the camera network $\mathcal{G}$, where $\mathcal{V}_{\mathrm{d}} = \mathcal{V}$, and $(i,j) \in \mathcal{E}_{\mathrm{d}}$ if and only if $(i,j) \in \mathcal{E}$ and $i < j$. For each $(i,j) \in \mathcal{E}_{\mathrm{d}}$, let $\eta_{ij} \in \mathcal{O}_p$ be the *relative measurement* between camera i and camera j, that is $\eta_{ij} = \theta_i - \theta_j$. Let θ be the vector of the cameras orientations, and let η be the vector of relative measurements. Assign an arbitrary ordering to the edges $\mathcal{E}_{\mathrm{d}}$, and define the incidence matrix $B \in \mathbb{F}_{\mathrm{p}}^{m \times n}$ of $\mathcal{G}_{\mathrm{d}}$ by specifying the k-row of B corresponding to the edge (i,j) as

$$b_{k\ell} = \begin{cases} 1, & \text{if } \ell = i, \\ -1, & \text{if } \ell = j, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Observe that $B\theta = \eta$. We consider the problem of finding cameras orientations θ to satisfy $B\theta = \eta$ over $\mathbb{F}_{\mathrm{p}}$ given the relative measurements η. For this problem in Algorithm 1 we propose an algorithm that requires each camera to have access to local relative measurements and to communicate with its immediate neighbors.

Because cameras transmit and operate only values in the finite field $\mathbb{F}_{\mathrm{p}}$, Algorithm 1 is suitable for cameras with limited capabilities, and robust to transmission noise.

Algorithm 1 *Distributed pose estimation (camera i)*

Input: Discretization accuracy p, Initial pose $\theta_i(0) \in \mathcal{O}_p$, Neighbors sets $\mathcal{N}_i^{\mathrm{in}}$ and $\mathcal{N}_i^{\mathrm{out}}$, Weights $a_{ij} \in \mathbb{F}_{\mathrm{p}}^{n \times n}$ for all $j \in \mathcal{N}_i^{\mathrm{in}}$, Number of iterations T (set $T = n$ otherwise), Relative measurements $\eta_{ij} \in \mathcal{O}_p$ for all $j \in \mathcal{N}_i^{\mathrm{in}}$;
Require: p is a prime number, $A = [a_{ij}]$ achieves average consensus over $\mathbb{F}_{\mathrm{p}}$;
Output: Orientation θ_i compatible with measurements $\eta = [\eta_{ij}]$;

for $t = 0, \dots, T$ **do**
Transmit $x_i(t) = \frac{p\theta_i(t)}{2\pi}$ to $\mathcal{N}_i^{\mathrm{out}}$;
Receive $x_j(t) = \frac{p\theta_j(t)}{2\pi}$ from $\mathcal{N}_i^{\mathrm{in}}$;
Update orientation $\theta_i(t)$ as:

$$x_i(t+1) = \sum_{j \in \mathcal{N}_i^{\mathrm{in}}} a_{ij} \left(x_j(t) + \frac{p\,\eta_{ij}}{2\pi} \right), \tag{6a}$$

$$\theta_i(t+1) = x_i(t+1)\frac{2\pi}{p}. \tag{6b}$$

end for
return Orientation θ_i;

Theorem 6.3 ***(Convergence of Algorithm 1 with perfect measurements)*** *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a camera network, and let $\mathcal{G}_{\mathrm{d}}$ be its associated directed graph. Let $\eta \in \mathcal{O}_p^m$ be the vector of relative measurements, and let B be the incidence matrix of $\mathcal{G}_{\mathrm{d}}$. If $\eta \in \mathrm{Im}(B)$ and A achieves average consensus over $\mathbb{F}_{\mathrm{p}}$, then*

(i) Algorithm 1 converges in finite time, that is, $\tilde{\theta} := \theta(T) = \theta(T+\tau)$ for some $\tilde{\theta} \in \mathcal{O}_p^n$, $T < n$, and for all $\tau \in \mathbb{N}$, and
(ii) the final network orientation is compatible with the relative measurements, that is, $B\tilde{\theta} = \eta$.

PROOF: Consider the update law (6a), and notice that it can be written as $x(t+1) = Ax(t) + LBv$, where $\frac{p}{2\pi}\eta = Bv$ for some vector $v \in \mathbb{F}_{\mathrm{p}}^n$ ($y \in \mathrm{Im}(B)$ by assumption), $L \in \mathbb{F}_{\mathrm{p}}^{n \times m}$, and the k-th column of L corresponding to the edge $(i,j) \in \mathcal{E}_{\mathrm{d}}$ is specified as

$$l_{\ell k} = \begin{cases} a_{ij}, & \text{if } \ell = i, \\ -a_{ij}, & \text{if } \ell = j, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Observe that

$$(LB)_{ij} = \begin{cases} \sum_{k \in \mathcal{N}_i^{\mathrm{in}}} a_{ik}, & \text{if } i = j, \\ -a_{ij}, & \text{if } j \in \mathcal{N}_i^{\mathrm{in}}, \\ 0, & \text{otherwise.} \end{cases}$$

so that $LB\mathbb{1} = 0$ (asymmetric Laplacian matrix of $\mathcal{G}$ [1]). Notice that $x(t) = A^t x(0) + \sum_{\tau=0}^{t-1} A^\tau LBv$. Since A

achieves average consensus, we have $A^T = n^{p-2}\mathbb{1}\mathbb{1}^\mathsf{T}$ for some $T < n$. Thus, $A^t LB = n^{p-2}\mathbb{1}\mathbb{1}^\mathsf{T} LB$ for all $t \geq T$. We now show that $\mathbb{1}^\mathsf{T} LB = 0$, from which statement (i) follows. Since A achieves average consensus, it follows from Theorem 6.1 that $A\mathbb{1} = \mathbb{1}$ and $\mathbb{1}^\mathsf{T} A = \mathbb{1}^\mathsf{T}$. Hence, for each node $k \in \mathcal{V}$, $\sum_{j=1}^n a_{kj} = \sum_{j=1}^n a_{jk}$, and, consequently, $\mathbb{1}^\mathsf{T} LB = 0$.

Let $\tilde{x}$ be a fixed point of (6a), that is, $(I - A)\tilde{x} = LBv$. Since $A\mathbb{1} = \mathbb{1}$, it follows that $I = \mathrm{diag}(\sum_j a_{1,j}, \ldots, \sum_j a_{n,j})$, and $I - A = LB$. Then $(I - A)(\tilde{x} - v) = LB(\tilde{x} - v) = 0$ for every fixed point $\tilde{x}$ of (6a). Because A is a consensus matrix, $A\mathbb{1} = \mathbb{1}$, and 1 is a simple eigenvalue of A. Then $\mathrm{Ker}(I - A) = \mathrm{Ker}(LB) = \mathrm{Im}(\mathbb{1})$, and $\tilde{x} - v \in \mathrm{Im}(\mathbb{1})$. Finally, since $\eta = \frac{2\pi}{p} Bv$, $\tilde{\theta} = \frac{2\pi}{p}\tilde{x}$, and $B\mathbb{1} = 0$, we conclude that $B\tilde{\theta} - \eta = \frac{2\pi}{p} B\,(\tilde{x} - v) = 0$. □

In Theorem 6.3 we assume that the measurements satisfy $\eta \in \mathrm{Im}(B)$ or, equivalently, that the measurements are not affected by noise. We next study the evolution of Algorithm 1 when $\eta \notin \mathrm{Im}(B)$. Let $e(t) = \eta - B\theta(t)$.

Theorem 6.4 ***(Convergence of Algorithm 1 with noisy measurements)*** *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a camera network, and let $\mathcal{G}_\mathrm{d}$ be its associated directed graph. Let $\eta \in \mathcal{O}_p^m$ be the vector of relative measurements, and let B be the incidence matrix of $\mathcal{G}_\mathrm{d}$. If A achieves average consensus over $\mathbb{F}_\mathrm{p}$, then*

(i) there exists a finite time $T < n$ such that the estimation error is constant, that is, $e(t) = e(t+1)$ for all $t \geq T$, and
(ii) for all $t \geq T$, the estimation error satisfies

$$e(t) = \left(I - B \sum_{\tau=0}^{T-1} A^\tau L \right) \eta_\mathrm{orth},$$

where η_orth is the orthogonal projection of η onto $\mathrm{Im}(B)^\perp$, and L is as in (7).

PROOF: With the same notation as in the proof of Theorem 6.3, let $T < n$ be the number of iterations needed for convergence of the network matrix A, that is, $A^T = n^{p-2}\mathbb{1}\mathbb{1}^\mathsf{T}$. Notice that $BA^t = 0$ for all $t \geq T$, so that

$$e(t) = \eta - B\left(A^t\theta(0) - \sum_{\tau=0}^{t-1} A^\tau L\eta \right) = \eta - B\sum_{\tau=0}^{T-1} A^\tau L\eta,$$

for all $t \geq T$, and statement (i) follows. To show statement (ii), let $\eta = \eta_\mathrm{par} + \eta_\mathrm{orth}$, where $\eta_\mathrm{par} \in \mathrm{Im}(B)$, and $\eta_\mathrm{orth} \in \mathrm{Im}(B)^\perp$. From the linearity of (6a) and Theorem 6.3 we have

$$\eta_\mathrm{par} = B \sum_{\tau=0}^{T-1} A^\tau L\eta_\mathrm{par},$$

which concludes the proof. □

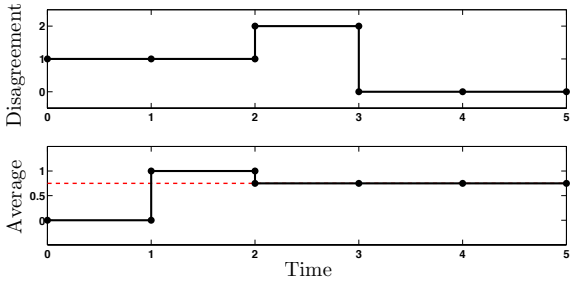

Fig. 5. For the network described by the matrix A in Example 7, let $0, 1, 1, 1$ be the agents initial states, respectively. Agents implement the algorithm described in Section 6.1. In the figure above we report the network disagreement as a function of time, where the disagreement at a given time equals the largest agents state minus the smallest agents state. Notice that the network achieves consensus in 3 iterations (see Section 4). In the figure below we report the average computed by the first agent (solid black) as a function of time (see Section 6.1). Notice that the first agent, and hence every agent in the network, computes the average of the initial states (dashed red) at the third iteration.

Theorem 6.4 characterizes the performance of Algorithm 1 when the measurements are affected by noise. Notice that the estimation error can be minimized by properly choosing the network matrix A.

Example 7 ***(Average computation and pose estimation via finite-field consensus)*** *Consider a camera network with 4 cameras configured in a circle topology and network matrix $A = \begin{bmatrix} 0 & 4 & 2 & 0 \\ 1 & 1 & 0 & 4 \\ 0 & 0 & 2 & 4 \\ 0 & 1 & 2 & 3 \end{bmatrix} \in \mathbb{F}_5^{4\times 4}$. It can be verified that A achieves average consensus over $\mathbb{F}_5$ in at most 3 iterations. In Fig. 5 we show that the network matrix A allows for the computation of the real-valued average of the agents initial states in 3 iterations.*

Let $A_\mathrm{k} \in \mathbb{F}_5^{1024\times 1024}$ be the network matrix generated from A as $A_\mathrm{k} = A \otimes A \otimes A \otimes A \otimes A$. In Fig. 6 we validate our distributed pose estimation algorithm. □

7 Conclusion and Future Work

In this paper we propose a distributed consensus algorithm for agents with limited memory, computation, and communication capabilities. Our approach is based on finite-fields, where agents states lie in a finite set, and

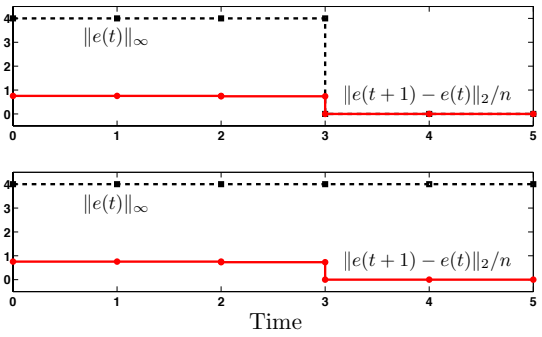

Fig. 6. For the camera network with 1024 cameras described by the matrix A_{k} in Example 7, this figure show the effectiveness of Algorithm 1. The figure above considers the noiseless case (Theorem 6.3). The dashed black line denotes the infinity norm of the estimation error, while the solid red line corresponds to the (normalized) two norm of the difference between two consecutive estimation errors. We conclude that, in the absence of measurement noise, Algorithm 1 converges in 3 iterations to a configuration compatible with the relative measurements. The figure below considers the case of noisy measurements (Theorem 6.4). The estimation error remains nonzero (dashed black). However, the algorithm converges to a configuration with constant estimation error, as the difference between two consecutive estimation errors is zero after 3 iterations (solid red).

operations are performed according to modular arithmetic. For our algorithm we identify necessary and sufficient convergence conditions, and we characterize the convergence time. Additionally, we discuss several network design methods, and we propose some application scenarios. Our work proposes a class of consensus dynamics, which are advantageous in several applications, and it complements the existing literature on consensus.

Through our analysis we show that finite-field consensus networks outperforms their real-valued counterpart in many aspects, including the convergence speed, robustness to communication errors, and agents requirements. These advantages come at the expenses of a more convoluted network design, which we identify as an interesting research direction. In particular, distributed network design algorithms, as well as gossip and asynchronous protocols should be investigated to broaden the applicability of finite-field consensus networks. Other theoretical research questions include characterizing the existence of finite-field consensus weights for a given interconnection structure and field characteristic, as well as the design of fastest finite-field consensus networks with fixed agents interconnection graph.

APPENDIX

Due to space constraint, we refer the reader to [18], [17], and [20] for fundamental results and facts in linear algebra, including the Primary Decomposition Theorem, the order of polynomial over a field, and the cycle structure of the transition graph of an iteration over a finite field.

PROOF of Theorem 4.3: Let $P_A \in \mathbb{F}_{\mathrm{p}}[s]$ be the characteristic polynomial of A, and notice that P_A can be written as $P_A(s) = \det(sI - A) = s^h \bar{P}(s)$, for some $h \in \mathbb{N}_{\geq 0}$, and $\bar{P}(s) \in \mathbb{F}_{\mathrm{p}}[s]$ with $\bar{P}(0) \neq 0$.

(i) $\implies$ *(ii)* Since A is row-stochastic, $1 \in \sigma_{\mathrm{p}}(A)$. Thus, we factorize P_A in irreducible polynomials as

$$P_A(s) = (s-1)^k \prod_{j=1}^{r} Q_j(s)^{m_j},$$

where $k, m_j \in \mathbb{N}$ are given by the algebraic multiplicity of the corresponding eigenvalue.

We start by showing that $k = 1$. Assume by contradiction that $k > 1$. Let $\mathcal{W}_2 = \mathrm{Ker}((I-A)^k)$, and let A_2 be the restriction of A to $\mathcal{W}_2$. Recall from [20] that the cycle structure of the transition graph $\mathcal{G}_2$ of A_2 is

$$\mathrm{Cycles}(\mathcal{G}_2) = C_1 + \sum_{i=1}^{k} (p^i - p^{i-1}) C_1, \qquad \text{(A-1)}$$

where the sums of cycles is just the corresponding union graph, and C_1 denotes a unit cycle, that is, a fixed point for A. From (A-1) it follows that, if $k > 1$, then the number of cycles in $\mathcal{G}_2$ is strictly greater than p. By Theorem 4.1 we conclude that $k = 1$.

We now show that $r = 0$. Assume by contradiction that $r > 0$. Let $\mathcal{W}_3 = \mathrm{Ker}(Q_j(A)^{m_j})$, and let A_3 be the restriction of A to $\mathcal{W}_3$. The cycle structure of the transition graph $\mathcal{G}_3$ of A_3, that is the set of cycles of $\mathcal{G}_3$ [20], is

$$\mathrm{Cycles}(\mathcal{G}_3) = C_1 + \sum_{i=1}^{m_j} \frac{p^{\deg(Q_j)i} - p^{\deg(Q_j)(i-1)}}{\ell_i} C_{\ell_i},$$

where $\ell_i = \mathrm{ord}(Q_j^{n_j}) \geq \deg(Q_j) \geq 1$ from [17], $\deg(\cdot)$ denotes the degree of a polynomial, and C_ℓ is a cycle of length ℓ. Since the graph structure of A is given by the product of the graphs associated with the irreducible factors of its characteristic polynomial [20], the number of cycles is greater than p whenever $k > 1$ or $r > 0$ (see Example 4 and Fig. 2).

(ii) $\implies$ *(i)* Let $\mathcal{W}_1 = \mathrm{Ker}(A - I) = \mathrm{Im}(\mathbb{1})$. Due to the Primary Decomposition Theorem in linear algebra [18], $\mathcal{W}_1$ is A-invariant. Let $V = [V_1 \; \mathbb{1}]$ be an invertible matrix, where the columns of V_1 are a basis for $\mathcal{W}_1^\perp$. Then we have $\tilde{A} = V^{-1}AV = \left[\begin{smallmatrix} A_{11} & 0 \\ A_{21} & 1 \end{smallmatrix}\right]$. Since the eigenvalues of a matrix are not affected by similarity transformations, the characteristic polynomial of the matrix A_{11} is s^{n-1}, so that A_{11} is nilpotent. It follows that every vector in $\mathcal{W}_1^\perp$ converges to the origin in at most $n-1$ iterations, while vectors in $\mathcal{W}_1$ (consensus vectors) are fixed points for the matrix A. $\square$

References

[1] F. Bullo, J. Cortés, and S. Martínez. *Distributed Control of Robotic Networks*. Princeton University Press, 2009.

[2] F. Garin and L. Schenato. A survey on distributed estimation and control applications using linear consensus algorithms. In A. Bemporad, M. Heemels, and M. Johansson, editors, *Networked Control Systems*, LNCIS, pages 75–107. Springer, 2010.

[3] W. Ren, R. W. Beard, and E. M. Atkins. Information consensus in multivehicle cooperative control: Collective group behavior through local interaction. *IEEE Control Systems Magazine*, 27(2):71–82, 2007.

[4] L. Xiao, S. Boyd, and S. Lall. A scheme for robust distributed sensor fusion based on average consensus. In *Symposium on Information Processing of Sensor Networks*, pages 63–70, Los Angeles, CA, USA, April 2005.

[5] D. P. Bertsekas and J. N. Tsitsiklis. *Parallel and Distributed Computation: Numerical Methods*. Athena Scientific, 1997.

[6] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1996.

[7] Y. G. Sun, L. Wang, and G. Xie. Average consensus in networks of dynamic agents with switching topologies and multiple time-varying delays. *Systems & Control Letters*, 57(2):175–183, 2008.

[8] T. C. Aysal, M. E. Yildiz, A. D. Sarwate, and A. Scaglione. Broadcast gossip algorithms for consensus. *IEEE Transactions on Signal Processing*, 57(7):2748–2761, 2009.

[9] S. Kar and J. M. F. Moura. Distributed consensus algorithms in sensor networks with imperfect communication: Link failures and channel noise. *IEEE Transactions on Signal Processing*, 57(1):355–369, 2009.

[10] L. Moreau. Stability of multiagent systems with time-dependent communication links. *IEEE Transactions on Automatic Control*, 50(2):169–182, 2005.

[11] A. Nedić, A. Olshevsky, A. Ozdaglar, and J. N. Tsitsiklis. On distributed averaging algorithms and quantization effects. *IEEE Transactions on Automatic Control*, 54(11):2506–2517, 2009.

[12] T. Li, M. Fu, L. Xie, and J. F. Zhang. Distributed consensus with limited communication data rate. *IEEE Transactions on Automatic Control*, 56(2):279–292, 2011.

[13] A. Fagiolini, E. M. Visibelli, and A. Bicchi. Logical consensus for distributed network agreement. In *IEEE Conf. on Decision and Control*, pages 5250–5255, Cancún, México, December 2008.

[14] A. Kashyap, T. Başar, and R. Srikant. Quantized consensus. *Automatica*, 43(7):1192–1203, 2007.

[15] S. Sundaram and C. Hadjicostis. Structural controllability and observability of linear systems over finite fields with applications to multi-agent systems. *IEEE Transactions on Automatic Control*, 58(1):60–73, 2013.

[16] R. Koetter and M. Médard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, 2003.

[17] B. Elspas. The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, 6(1):45–60, 1959.

[18] G. Shilov. *Linear Algebra*. New York: Dover Publications, 1977.

[19] C. D. Godsil and G. F. Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer, 2001.

[20] R. A. H. Toledo. Linear finite dynamical systems. *Communications in Algebra*, 33(9):2977–2989, 2005.

[21] J. C. Delvenne, R. Carli, and S. Zampieri. Optimal strategies in the average consensus problem. In *IEEE Conf. on Decision and Control*, New Orleans, USA, December 2007.

[22] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1994.

[23] P. Singla. On representations of general linear groups over principal ideal local rings of length two. *Journal of Algebra*, 324(9):2543–2563, 2010.

[24] R. Olfati-Saber and R. M. Murray. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, 49(9):1520–1533, 2004.

[25] A. S. Fraenkel and Y. Yesha. Complexity of problems in games, graphs and algebraic equations. *Discrete Applied Mathematics*, 1(1-2):15–30, 1979.

[26] J. Ding, J. E. Gower, and D. Schmidt. *Multivariate Public Key Cryptosystems*. Springer, 2006.

[27] L. Bettale, J. C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009.

[28] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 392–407. Springer, 2000.

[29] P. M. Weichsel. The Kronecker product of graphs. *Proceedings of the American Mathematical Society*, 13(1):47–52, 1962.

[30] S. Mac Lane. Modular fields. *The American Mathematical Monthly*, 47(5):259–274, 1940.

[31] G. Piovan, I. Shames, B. Fidan, F. Bullo, and B. D. O. Anderson. On frame and orientation localization for relative sensing networks. *Automatica*, 49(1):206–213, 2013.