Synchronization of networks over finite fields [⋆]

Min Meng, Xiuxian Li, Gaoxi Xiao

School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798

Abstract

In this paper, the synchronization problem for networks over finite fields is investigated, which is a generalization of consensus and provides a new perspective for networks of agents with limited capacities of memory and communication. It is assumed that the states and communication weights can only attain values from a finite alphabet equipped with a prime number of integers, termed finite fields, and operations are processed relying on modular arithmetic. For this synchronization problem, necessary and sufficient conditions are derived based on the transition graph of the studied network. The large number of nodes in the transition graph, dependent on the numbers of integers in finite fields and the agents, may lead to high computational cost and difficulties in verifying synchronization. To avoid this, an equivalent condition for synchronization of networks is provided by the characteristic polynomial of the studied network matrix. Furthermore, in a synchronized network over finite fields, the periodic behavior can be determined by the network matrix and the initial state.

Key words: Synchronization, networks, finite fields, graph theory.

1 Introduction

For multi-agent systems, the problem of synchronization/consensus among individual agents aiming to agree on a common goal of interest by communicating local information, i.e., the information of the agents' neighbors, is one of the fundamental and interesting issues in cooperative control. This problem has attracted much attention during recent years because of its wide applications in different areas, such as robotics (Ren, Beard & Atkins 2007), power networks (Rahbari-Asr et al. 2014), sensor networks (Hong & Scaglione 2005), to name just a few. Up to now, there have been a great many results on synchronization/consensus of multi-agent networks under time-delayed/time-varying communication topologies (Garcia et al. 2017, Meng, Liu & Feng 2018, Nuno et al. 2011, Olfati-Saber & Murray 2004, Proskurnikov 2013, Wang, Zhu & Feng 2019), networks with nonlinear dynamics (Li, Liu & Feng 2018, Liu et al. 2018, Liuzza et al. 2016), networks under adversary environments (Feng, Hu & Wen 2016, Feng, Wen & Hu 2017, LeBlanc & Koutsoukos 2018, Moghadam et al. 2018) and so on.

Compared with multi-agent systems processing and transiting real numbers, the cases where states of networks attain values from finite sets are more realistic in dealing with limited storage capacities and communication bandwidths (Fagiolini & Bicchi 2013, Kashyap, Başar & Srikant 2007). Recently, such cases are formulated by virtue of the concept of finite fields in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014), Sundaram & Hadjicostis (2013), Xu & Hong (2014). In these references, the state of each agent in the studied network is considered to take a value from a finite field and update its value by a modular-arithmetic-based sum of the neighbors' states. Such a network can have a finite convergence time due to its finite states, and thus is appropriate for capacity and memory limited cases subject to constrained time. An earliest work on finite field consensus was presented in Pasqualetti, Borra & Bullo (2014), in which several necessary and sufficient conditions were derived on the basis of the transition graph and the characteristic polynomial of the network matrix. The applications to average consensus in real numbers and pose estimation in sensor networks were also discussed. Subsequently, leader-following consensus of multi-agent systems with dynamics of high dimensions over finite fields was studied in Xu & Hong (2014). Li et al. (2016), Li, Su & Chen (2016) extended the finite field consensus results in Pasqualetti, Borra & Bullo (2014) to the networks with switching topologies and time-delays. On the other hand, a new approach was presented in Li, Zhao & Guo (2018), Li et al. (2019) to study consensus of networks over finite fields by converting the n-dimensional network system to a

[⋆] The work was partially supported by Ministry of Education, Singapore, under contract of MOE2016-T2-1-119. Corresponding author: Gaoxi Xiao.

Email addresses: minmeng@ntu.edu.sg (Min Meng), xiuxianli@ntu.edu.sg (Xiuxian Li), egxxiao@ntu.edu.sg (Gaoxi Xiao).

p^n-dimensional system via the semi-tensor product. In the existing researches on finite field consensus, it is required that the states of the studied network over finite fields reach a common value and stay at the value permanently, that is, consensus at a fixed value. This requires that the network matrix has to be a row-stochastic or a nilpotent matrix (Pasqualetti, Borra & Bullo 2014). However, reaching a fixed value may not be applicable for some practical systems. For example, in a network of robotic manipulators, the goal is to carry a subject from one place to another. By taking the subject as a single point, all the manipulators should be largely ensured to reach the same time-varying position. That is to make the positions of the manipulators achieve synchronization rather than reaching a fixed position. As the methods and results in Pasqualetti, Borra & Bullo (2014) are not applicable to solving the synchronization problem, open issues remain in dealing with multi-agent networks over finite fields.

In this paper, we study the synchronization problem of networks over finite fields. The main contributions are summarized as follows. i) We obtain that synchronization of networks over finite fields has intrinsically different characteristics from those of consensus of networks over finite fields. A necessary condition on the iteration network matrices is obtained for a synchronized network over finite fields (Lemma 2). And we obtain that there is only a unit cycle around $\mathbf{0}_n$ and several other cycles of equal length in the associated transition graph of a synchronized network over finite fields (Theorem 2), while there are only unit cycles in the corresponding transition graph for a consensus network (Pasqualetti, Borra & Bullo 2014). Further, the network matrix has a nonzero eigenvalue, which is equal to its row sum (Theorem 3) and may not be 1. ii) Based on Jordan decomposition, in a synchronized network, the cycle, which can be reached from a given initial state in finite time, is determined (Theorem 4). This finite time is not more than the largest dimension of the Jordan block associated with the eigenvalue 0 of the network matrix.

The rest of this paper is organized as follows. In Section 2 some necessary preliminaries and existing results, as well as the problem formulation, are introduced. Section 3 devotes to deriving several necessary and sufficient conditions for synchronization of networks over finite fields based on the transition graph and network iteration matrix. Section 4 makes a brief conclusion.

2 Preliminaries and problem formulation

In this section, some definitions about finite fields and algebraic graph theory, along with the problem formulation, are introduced.

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

- (Closure under addition and multiplication) For arbitrary two elements $\mu, \nu \in \mathbb{F}$, one has $\mu + \nu \in \mathbb{F}$ and $\mu \cdot \nu \in \mathbb{F}$.
- (Associativity of addition and multiplication) For any $\mu, \nu, \omega \in \mathbb{F}$, $\mu + (\nu + \omega) = (\mu + \nu) + \omega$ and $\mu \cdot (\nu \cdot \omega) = (\mu \cdot \nu) \cdot \omega$ hold.
- (Commutativity of addition and multiplication) For any $\mu, \nu \in \mathbb{F}$, $\mu + \nu = \nu + \mu$ and $\mu \cdot \nu = \nu \cdot \mu$.
- (Existence of additive and multiplicative identity elements) For any $\mu \in \mathbb{F}$, there exist two elements 0 (additive identity element) and 1 (multiplicative identity element) in $\mathbb{F}$ such that $\mu + 0 = \mu$ and $\mu \cdot 1 = \mu$.
- (Existence of additive and multiplicative inverse elements) For any $\mu \in \mathbb{F}$, there exist two elements ν (additive inverse element) and ω (multiplicative inverse element) in $\mathbb{F}$ such that $\mu + \nu = 0$ and $\mu \cdot \omega = 1$ when $\mu \neq 0$.
- (Distributivity of multiplication over addition) For any $\mu, \nu, \omega \in \mathbb{F}$, it holds that $\mu \cdot (\nu + \omega) = \mu \cdot \nu + \mu \cdot \omega$.

A field $\mathbb{F}$ is finite if the number of the elements in $\mathbb{F}$ is finite. The fundamental concepts and properties about finite fields can be referred to Lidl & Niederreiter (1997). In this paper, we consider a type of finite fields, prime fields with a prime number of elements. In the field $\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\}$, where p is a prime number, the addition and multiplication are defined in modular arithmetic, i.e., performing the corresponding operations over the integer field $\mathbb{Z}$ and taking the remainder after divided by p.

Lemma 1 (Lidl & Niederreiter (1997)) *(*Fermat's Little Theorem*) Let p be a prime number. Then for arbitrary integer α not divisible by p, it holds that p divides $\alpha^{p-1} - 1$, i.e., $p | (\alpha^{p-1} - 1)$.*

Denote by $\mathscr{G} = (\mathscr{V}_n, \mathscr{E}, A)$ be a directed graph with the vertex set $\mathscr{V}_n = \{v_1, v_2, \ldots, v_n\}$, the directed edge set $\mathscr{E}$ and the weighted adjacency matrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$. Let (v_i, v_j) represent the directed edge in $\mathscr{E}$ from node v_i to node v_j, and node v_i is termed a parent node of v_j and node v_j is called a child node of v_i. A graph is said to be undirected if $(v_i, v_j) \in \mathscr{E}$ implies $(v_j, v_i) \in \mathscr{E}$. The weights are defined as $a_{ij} > 0$ if $(v_j, v_i) \in \mathscr{E}$ and $a_{ij} = 0$ otherwise. Self-loops are allowed in the graph $\mathscr{G}$. For node v_i, the in-degree and out-degree of v_i are, respectively, the numbers of elements in in-neighbor set $\mathscr{N}_i^+ = \{v_j \mid (v_j, v_i) \in \mathscr{E}\}$ and out-neighbor set $\mathscr{N}_i^- = \{v_j \mid (v_i, v_j) \in \mathscr{E}\}$. A node v_i has unit out-degree (resp. in-degree) if and only if the number of elements in $\mathscr{N}_i^-$ (resp. $\mathscr{N}_i^+$) is one. A directed path from node v_{j_1} to node v_{j_l} is composed of a sequence of ordered edges $(v_{j_i}, v_{j_{i+1}})$, $i = 1, 2, \ldots, l-1$. A cycle is a path in which only the first and last vertices in the path sequence are the same. The length of a path (resp. cycle) is the number of edges in the path (resp. cycle). The directed graph is said to be strongly (resp. weakly) connected if there is a directed (resp. an undirected) path between any two nodes. A globally reachable node is a node to which there are directed paths from all the nodes in this graph. Two subgraphs of a graph are disjoint if there are no common nodes in the two subgraphs.

The notation $\mathbf{1}_n$ (resp. $\mathbf{0}_n$) represents an n-dimensional vector with every element being 1 (resp. 0). Here, 1 and 0 are, respectively, multiplicative identity element and additive identity element in the finite field $\mathbb{F}_p$. Over finite field $\mathbb{F}_p$, an $n \times n$ matrix B is called a row-stochastic matrix if the sum of all the elements in every row of B is equal to 1, i.e., $B\mathbf{1}_n = \mathbf{1}_n$, and is called a nilpotent matrix if there exists a positive integer c such that B^c is the zero matrix.

In what follows, we dedicate to introducing our studied problem. Consider a network with n agents operating over a finite field $\mathbb{F}_p$, where p is a prime number. Assume that the communication topology among the n agents is a directed graph $\mathscr{G} = (\mathscr{V}_n, \mathscr{E}, A)$ with $\mathscr{V}_n = \{1, 2, \dots, n\}$ being the set of n agents, and then the dynamics of the ith agent is described as follows:

$$x_i(t+1) = \sum_{j \in \mathscr{N}_i^+} a_{ij} x_j(t), \tag{1}$$

where $x_i(t) \in \mathbb{F}_p$ is the state of agent i, $i = 1, 2, \dots, n$, and the edge weight a_{ij} is in $\mathbb{F}_p$, i.e., $A = (a_{ij}) \in \mathbb{F}_p^{n\times n}$. Let $x(t) = (x_1(t), x_2(t), \dots, x_n(t))^T$, then the dynamics of the network can be rewritten as

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

The transition graph associated with network (2) over $\mathbb{F}_p$ is defined as $\mathscr{G}_A = (\mathscr{V}_A, \mathscr{E}_A)$ with the vertex set $\mathscr{V}_A = \{v \mid v \in \mathbb{F}_p^n\}$ and the edge set $\mathscr{E}_A = \{(v_i, v_j) \mid v_j = Av_i, \forall v_i, v_j \in \mathscr{V}_A\}$. It should be noted that the transition graph $\mathscr{G}_A$ possesses several properties: a) it contains exactly p^n vertices and p^n directed edges; b) each vertex in $\mathscr{G}_A$ has unit out-degree; c) it is composed of disjoint weakly connected subgraphs, each of which contains only one cycle and embraces a globally reachable node (Hernández Toledo 2005, Li, Su & Chen 2016, Pasqualetti, Borra & Bullo 2014). To proceed, the definition of synchronization of network (2) over the finite field $\mathbb{F}_p$ is firstly given as follows.

Definition 1 *The network (2) over $\mathbb{F}_p$ achieves synchronization if for any initial state $x(0) \in \mathbb{F}_p^n$, there exists a finite time $K \in \mathbb{N}$ such that $x_1(t) = x_2(t) = \cdots = x_n(t)$ for all $t \geq K$.*

Remark 1 *As defined in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014), network (2) over $\mathbb{F}_p$ achieves consensus if for any initial state $x(0) \in \mathbb{F}_p^n$, there exists a finite time $K \in \mathbb{N}$ such that $x(K) = x(K+t) = \gamma\mathbf{1}_n$ for some $\gamma \in \mathbb{F}_p$ and all $t \in \mathbb{N}$. The states of a consensus network over finite fields will reach a common value and stay at the value forever, while the states of a synchronized network over finite fields will be equal to each other, not necessarily remaining at a fixed value. In literature on multi-agent systems, consensus and synchronization are often used interchangeably.*

Remark 2 *Similar to the claim for consensus networks over finite fields, synchronization of network (2) over finite fields can converge in finite time due to its finite states, a feature that is not always achieved over the field of real numbers.*

Example 1 *In this example, we consider the network (2) over the finite field $\mathbb{F}_5$ with the network matrix as*

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

It is easy to see that $A\mathbf{1}_3 = 4\mathbf{1}_3$, and thus A is not a row-stochastic matrix or nilpotent matrix. Based on the consensus definition and results in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014), which require the network matrix to be row-stochastic or nilpotent, consensus of network (2) over $\mathbb{F}_5$ cannot be achieved. However, synchronization of network (2) over $\mathbb{F}_5$ based on Definition 1 can be achieved.

One equivalent condition to achieve synchronization of network (2) over $\mathbb{F}_p$ is that the state trajectory of (2) will enter and stay in the set $\Omega = \{\alpha\mathbf{1}_n | \alpha \in \mathbb{F}_p\}$. We conclude this section with a lemma that gives a necessary condition for achieving synchronization of networks over finite fields.

Lemma 2 *Consider the network in (2) over the finite field $\mathbb{F}_p$. If synchronization of network (2) is achieved, then either A is a nilpotent matrix or the row sums of A are the same and nonzero.*

Proof. As the network in (2) over $\mathbb{F}_p$ achieves synchronization, there exists a nonnegative integer K such that $x(t) \in \Omega$ for all $t \geq K$. Assume that $x(t) = \alpha\mathbf{1}_n$ and $x(t+1) = \beta\mathbf{1}_n$ for one $t \geq K$. Based on the iteration in (2), it can be obtained that $\beta\mathbf{1}_n = \alpha A\mathbf{1}_n$. In order to derive the constraints on matrix A, four cases are next discussed.

i) If $\alpha \neq 0$ and $\beta \neq 0$, then $A\mathbf{1}_n = \frac{\beta}{\alpha}\mathbf{1}_n$, which indicates that the row sums of A are the same and nonzero.

ii) If $\alpha = 0$ and $\beta \neq 0$, then $\beta\mathbf{1}_n = \alpha A\mathbf{1}_n$ yields that $\beta = 0$, which is a contradiction.

iii) If $\alpha \neq 0$ and $\beta = 0$, then $A(\gamma\mathbf{1}_n) = \mathbf{0}_n$ for all $\gamma \in \mathbb{F}_p$. Hence A is nilpotent since there exists a positive integer $\tilde{t}$ such that $x(\tilde{t}) = A^{\tilde{t}}x(0) = \mathbf{0}_n$ for any $x(0) \in \mathbb{F}_p$.

iv) If $\alpha = \beta = 0$, we should choose another time instant such that the above three cases hold. If the above three cases cannot happen, the synchronization implies that $x(t) = \mathbf{0}_n$ for all $t \geq K$. Then A is a nilpotent matrix.

In summary, if synchronization of network (2) over $\mathbb{F}_p$ is achieved, then either A is a nilpotent matrix or the row sums of A are the same and nonzero. ■

Remark 3 *From Definition 1 and Lemma 2, it can be claimed that finite field synchronization includes finite field consensus, which is defined in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014), as a special case. When $A\mathbf{1}_n = \mathbf{1}_n$, i.e., $\alpha = 1$, all the results for synchronization of networks over finite fields are degenerated to those in Pasqualetti, Borra & Bullo (2014).*

3 Main results

In this section, we devote to finding some necessary and sufficient conditions for achieving synchronization of network (2) over the finite field $\mathbb{F}_p$.

Theorem 1 *Consider network (2) over $\mathbb{F}_p$. Synchronization of network (2) over $\mathbb{F}_p$ is achieved if and only if for any initial state $x(0) \in \{e_{i,n} \mid i = 1,2,\dots,n\}$, where $e_{i,n}$ is an n-dimensional vector with the ith element being 1 and others 0, there exists a finite time $K \in \mathbb{N}$ such that $x_1(t) = x_2(t) = \cdots = x_n(t)$ for all $t \geq K$.*

Proof. The necessity is obvious from Definition 1. It suffices to prove the sufficient part. Note that each term $A^t e_{i,n}$ corresponds to the state at time t under the initial state $x(0) = e_{i,n}$. If the condition in the theorem holds, then one can get that for $t \geq K$,

$$A^t e_{i,n} \in \Omega = \{\alpha \mathbf{1}_n \mid \alpha \in \mathbb{F}_p\},\ i = 1,2,\dots,n. \tag{3}$$

For the vector space $\mathbb{F}_p^n$, $\{e_{i,n} \mid i = 1,2,\dots,n\}$ can be regarded as a basis. Thus for any initial state $x(0) = x_0 \in \mathbb{F}_p^n$, there exist n numbers $k_1, k_2, \dots, k_n$ in $\mathbb{F}_p$ such that

$$x_0 = k_1 e_{1,n} + k_2 e_{2,n} + \cdots + k_n e_{n,n}. \tag{4}$$

Then the state at time t corresponding to initial state $x(0) = x_0$ is

$$x(t) = A^t x_0 = k_1 A^t e_{1,n} + k_2 A^t e_{2,n} + \cdots + k_n A^t e_{n,n}.$$

By (3), $x(t) \in \Omega$ for $t \geq K$, that is, synchronization of network (2) over $\mathbb{F}_p$ is achieved. ■

Example 2 *Recall Example 1. The state trajectories under initial states $e_{1,3}$, $e_{2,3}$, $e_{3,3}$, respectively, are (see Fig. 1):*

$$\begin{aligned}
&e_{1,3} \to (2,2,2)^T \to (3,3,3)^T \to (2,2,2)^T \to \cdots \\
&e_{2,3} \to (1,2,2)^T \to (1,1,1)^T \to (4,4,4)^T \to (1,1,1)^T \to \cdots \\
&e_{3,3} \to (1,0,0)^T \to (2,2,2)^T \to (3,3,3)^T \to (2,2,2)^T \to \cdots
\end{aligned}$$

which implies that from any initial state in $\{e_{1,3}, e_{2,3}, e_{3,3}\}$, there exits a finite time K such that the state satisfies $x_1(t) = x_2(t) = x_3(t)$ for all $t \geq K$. Therefore, by Theorem 1, one can conclude that the network with iteration matrix A given in Example 1 can achieve synchronization.

From Theorem 1, one can easily verify whether network (2) over $\mathbb{F}_p$ achieves synchronization from the n initial states instead of the whole vector space $\mathbb{F}_p^n$. However, the detailed properties about the state trajectories and the synchronized value from any given initial state are not clear. Recalling Lemma 2, we limit our attention to the network matrices with the same and nonzero row sums, since the case where network matrices are nilpotent can always achieve synchronization/consensus at the value $\mathbf{0}_n$, independent of the initial states of the agents, and is thus trivial. As discussed in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014), to achieve consensus of networks over finite fields requires more stringent conditions than that of networks over real numbers. This statement is still true for synchronization of networks over the finite field $\mathbb{F}_p$. That is to say, the conditions on the topology graphs are not sufficient to ensure synchronization of network (2) over finite fields. In what follows, we discuss synchronization of network (2) over $\mathbb{F}_p$ from the perspective of its associated transition graph.

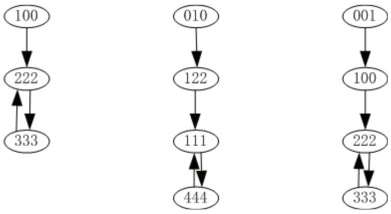

Fig. 1. The state trajectories corresponding to initial states $e_{1,3}$, $e_{2,3}$, $e_{3,3}$ of network (2) with A in Example 1.

Theorem 2 *Consider network (2) over $\mathbb{F}_p$. Assume that the row sums of network matrix A are the same and nonzero, and denote by $\mathscr{G}_A = (\mathscr{V}_A, \mathscr{E}_A)$ the transition graph of (2). Synchronization of network (2) over $\mathbb{F}_p$ is achieved if and only if there exists a positive integer r such that $\mathscr{G}_A$ contains only $r+1$ cycles, $C_0, C_1, \dots, C_r$, satisfying the following properties:*

i) C_0 is a unit cycle around $\mathbf{0}_n$, that is, C_0 is a cycle of length 1 and only contains the vertex $\mathbf{0}_n$;
ii) the vertex sets of $C_0, C_1, \dots, C_r$ constitute a partition of Ω;
iii) the lengths of $C_1, \dots, C_r$ are equal to each other.

Proof. *Necessity.* Since $A\mathbf{0}_n = \mathbf{0}_n$, i.e., $\mathbf{0}_n$ is a fixed point of A, there must be a unit cycle around $\mathbf{0}_n$ in the transition graph $\mathscr{G}_A$. Note that a state trajectory of (2) is in bijective correspondence with a path in $\mathscr{G}_A$ and every vertex in $\mathscr{G}_A$ has unit out-degree. If there are no other cycles in $\mathscr{G}_A$, i.e., there is only one unit cycle around $\mathbf{0}_n$ in $\mathscr{G}_A$, then there exists a directed path from any node in $\mathscr{G}_A$ to $\mathbf{0}_n$, which means that A is a nilpotent matrix. This contradicts that the row sums of A are the same and nonzero.

Next we prove that there exist r other cycles, $C_1, \dots, C_r$, satisfying conditions ii), iii). Without loss of generality, assume that $A\mathbf{1}_n = \alpha \mathbf{1}_n$, where $\alpha \in \mathbb{F}_p$ and $\alpha \neq 0$. Then, by the Fermat's little theorem in Lemma 1, the state trajectory under the initial state $x(0) = \mathbf{1}_n$ can be expressed as

$$\mathbf{1}_n \to \alpha \mathbf{1}_n \to \alpha^2 \mathbf{1}_n \to \cdots \to \alpha^{p-2} \mathbf{1}_n \to \mathbf{1}_n,$$

which is composed of a cycle, denoted by C_1. If the vertex set of C_1, denoted by $\mathscr{V}_1$, is equal to $\Omega \setminus \{\mathbf{0}_n\}$, then $r = 1$, and conditions ii), iii) are satisfied. If the vertex set $\mathscr{V}_1$ of C_1 is a proper subset of $\Omega \setminus \{\mathbf{0}_n\}$, then selecting one element $\alpha_2 \mathbf{1}_n \in \Omega \setminus (\{\mathbf{0}_n\} \cup \mathscr{V}_1)$, the state trajectory under the initial state $x(0) = \alpha_2 \mathbf{1}_n$ is

$$\alpha_2 \mathbf{1}_n \to \alpha_2 \alpha \mathbf{1}_n \to \alpha_2 \alpha^2 \mathbf{1}_n \to \cdots \to \alpha_2 \alpha^{p-2} \mathbf{1}_n \to \alpha_2 \mathbf{1}_n,$$

which consists of another cycle, denoted by C_2. Thus, the length of C_2 equals that of C_1. In addition, it holds that $\mathscr{V}_1 \cap \mathscr{V}_2 = \emptyset$ by the properties of the transition graph $\mathscr{G}_A$, where $\mathscr{V}_2$ is the vertex set of C_2. If $\mathscr{V}_1 \cup \mathscr{V}_2 = \Omega \setminus \{\mathbf{0}_n\}$, then $r = 2$, and conditions ii), iii) are satisfied. Otherwise, proceed with the above process. Since there are finite elements in Ω, one can always find a positive integer r number of cycles, $C_1, C_2, \dots, C_r$, satisfying conditions ii) and iii).

If there exists another cycle C, $C \neq C_i$, $i = 0, 1, 2, \dots, r$, then every vertex of C is not in Ω based on condition ii). This means there exists a trajectory of (2) which will not enter into the set Ω after any time. This leads to a contradiction to the synchronization of (2). The necessary part is proved.

Sufficiency. In view of the bijective correspondence between the trajectories of (2) and directed paths in its associated transition graph $\mathscr{G}_A$, we obtain that there exists a positive integer K such that for any initial state $x(0) \in \mathbb{F}_p^n$ and any $t \geq K$, $x(t) \in \Omega$. Hence, network (2) over $\mathbb{F}_p$ achieves synchronization. ■

In Theorem 2, the key point of the equivalent condition for synchronization of network (2) over $\mathbb{F}_p$ is on the r cycles not around $\mathbf{0}_n$. From the proof of Theorem 2, it can be seen that the length of C_i is the period of the periodic behaviors of the studied networks. Note that it cannot be claimed that the length of C_1 is $p-1$ since the trajectory $\mathbf{1}_n \to \alpha \mathbf{1}_n \to \alpha^2 \mathbf{1}_n \to \cdots \to \alpha^{p-2} \mathbf{1}_n \to \mathbf{1}_n$ may run through the cycle C_1 repeatedly. Therefore, a natural question is what is the relationship among r, p and α. To proceed, we introduce the concept of the order in elementary number theory (Burton 2006). Specifically, given two coprime integers a and b with $b > 1$, the *order* of a modulo b is the smallest positive integer k such that $a^k = 1 (\text{mod } b)$ (see Definition 8.1 in Burton (2006)). The following result shows how to compute r under p and α.

Proposition 1 *Consider network (2) over $\mathbb{F}_p$ and assume that the row sums of A are all equal to α ($\alpha \neq 0$). If the network (2) over $\mathbb{F}_p$ achieves synchronization, then*

i) the length s of C_i, $i = 1, 2, \dots, r$, in Theorem 2 is equal to the order of α modulo p;
ii) $s | (p-1)$ and $r = (p-1)/s$.

Proof. i) Since p is a prime number, α is coprime to p. Then the statement can be easily obtained from the proof of Theorem 2.

ii) By the Fermat's little theorem in Lemma 1, for nonzero $\alpha \in \mathbb{F}_p$, one has $\alpha^{p-1} = 1$. Hence $\alpha^s = 1$ indicates that $s | (p-1)$. On the other hand, by conditions ii) and iii) in Theorem 2, the number of cycles not around $\mathbf{0}_n$ in the corresponding transition graph $\mathscr{G}_A$ is $r = (p-1)/s$. ■

Remark 4 *Recalling Theorem 4.2 in Pasqualetti, Borra & Bullo (2014), a network over finite field $\mathbb{F}_p$ achieves consensus if and only if the corresponding transition graph has only p unit cycles around the vertices $\gamma \mathbf{1}_n$ for $\gamma \in \{0, 1, \dots, p-1\}$. There is no need to discuss the lengths or the number of the cycles, due to the unit length of the cycles in the transition graph. Consequently, from the results obtained above, synchronization of networks over finite fields defined in Definition 1 is intrinsically different from consensus of networks over finite fields in Li et al. (2016), Li, Su & Chen (2016), Pasqualetti, Borra & Bullo (2014).*

Example 3 *For the network in Example 1, one can compute that $A\mathbf{1}_3 = 4\mathbf{1}_3$, i.e., $\alpha = 4$. All the cycles in its associated transition graph $\mathscr{G}_A$ are $C_0 : \mathbf{0}_3$, $C_1 : \mathbf{1}_3 \rightleftarrows 4\mathbf{1}_3$, $C_2 : 2\mathbf{1}_3 \rightleftarrows 3\mathbf{1}_3$. Hence, the network in Example 1 over $\mathbb{F}_5$ achieves synchronization. Besides, in $\mathbb{F}_5$, the order s of $\alpha = 4$ modulo $p = 5$ is $s = 2$. Then the length of C_i is 2, and the number of cycles not around $\mathbf{0}_n$ is $r = (5-1)/2 = 2$.*

Remark 5 *From Theorem 2 and the fact that each vertex in the associated transition graph $\mathscr{G}_A$ has unit out-degree, $\mathscr{G}_A$ corresponds to a synchronized network that is composed of $(r+1)$ weakly connected subgraphs with the terminal nodes in the cycles $C_0, C_1, C_2, \dots, C_r$, respectively. By Proposition 3.4 in Hernández Toledo (2005), the structures of the transit parts (directed trees) are the same in the sense of isomorphism.*

Verifying synchronization of network (2) over $\mathbb{F}_p$ based on the condition in Theorem 2 may be prohibitive for large networks on account of the exponential growing in the size of the transition graph and the number of agents. In fact, there are p^n vertices and p^n edges in $\mathscr{G}_A$. Next, based on Theorem 2, we shall derive another equivalent condition for verifying synchronization of network (2) over $\mathbb{F}_p$ based on the network matrix instead of the transition graph.

Theorem 3 *Consider network (2) over $\mathbb{F}_p$. Assume that $A\mathbf{1}_n = \alpha \mathbf{1}_n$, where $\alpha \neq 0$. Then network (2) over $\mathbb{F}_p$ achieves synchronization if and only if the characteristic polynomial of A, denoted by $P_A(\lambda)$, is $P_A(\lambda) = \lambda^{n-1}(\lambda - \alpha)$.*

Proof. *Necessity*. Assume that the characteristic polynomial of A is

$$P_A(\lambda) = \lambda^h (\lambda - \alpha)^k \prod_{j=1}^{q} P_j(\lambda)^{m_j},$$

where $h \geq 0$, $k \geq 1$, $m_j \geq 0$, $P_j(\lambda) \neq 0$ when $\lambda \in \{0, \alpha\}$, and $P_j(\lambda)$ is an irreducible polynomial, $j = 1, 2, \dots, q$.

First, we prove $k = 1$. Assume by contradiction that $k > 1$. Let $W = \{v \in \mathbb{F}_p^n \mid (\alpha I_n - A)^k v = \mathbf{0}_n\}$ and $\mathscr{G}_{A|W}$ be a subgraph of $\mathscr{G}_A$ with the vertex set being W and the edge set being $\{(v_i, v_j) \mid (v_i, v_j) \in \mathscr{E}_A,\ v_i, v_j \in W\}$. By Theorem 5 in Hernández Toledo (2005), the cycle structure in the graph

$\mathscr{G}_{A_{|W}}$ is

$$C_0 + \sum_{i=1}^{k} \frac{p^i - p^{i-1}}{s_i} \tilde{C}_{s_i}, \tag{5}$$

where C_0 is the unit cycle around $\mathbf{0}_n$, $\tilde{C}_{s_i}$ is a cycle of length s_i, and the coeffident $(p^i - p^{i-1})/s_i$ before $\tilde{C}_{s_i}$ means that there are $(p^i - p^{i-1})/s_i$ cycles $\tilde{C}_{s_i}$ in $\mathscr{G}_{A_{|W}}$, $i = 1,2,\dots,k$. That is, the formula in (5) means that the graph $\mathscr{G}_{A_{|W}}$ has one unit cycle around $\mathbf{0}_n$ and $(p^i - p^{i-1})/s_i$ cycles of length s_i, $i = 1,2,\dots,k$. By Theorem 2, in $\mathscr{G}_A$, there are only those cycles of equal length s apart from the unit cycle around $\mathbf{0}_n$ and the vertex sets of all the cycles constitute the set $\Omega = \{\gamma \mathbf{1}_n \mid \gamma \in \mathbb{F}_p\}$. Note that $(\alpha I_n - A)^k \mathbf{1}_n = \mathbf{0}_n$ implying that $\Omega \subseteq W$. Then $\mathscr{G}_{A_{|W}}$ and $\mathscr{G}_A$ have the same cycles. Thus the cycle structure of $\mathscr{G}_{A_{|W}}$ becomes

$$C_0 + \frac{p-1}{s}\tilde{C}_s + \sum_{i=2}^{k} \frac{p^i - p^{i-1}}{s} \tilde{C}_s,$$

from which it is easy to see that the number of cycles in $\mathscr{G}_{A_{|W}}$ is greater than $1 + (p-1)/s$ when $k > 1$, which contradicts the result in Proposition 1. Hence, $k = 1$.

Similar to the proof of Theorem 4.3 in Pasqualetti, Borra & Bullo (2014), it can also be proved that $m_j = 0$, $j = 1,2,\dots,1$. Therefore, $P_A(\lambda) = \lambda^{n-1}(\lambda - \alpha)$.

Sufficiency. If the characteristic polynomial of A is $P_A = \lambda^{n-1}(\lambda - \alpha)$ and $A\mathbf{1}_n = \alpha \mathbf{1}_n$, then one can find a basis of the vector space $\mathbb{F}_p^n$ as $\mathbf{1}_n, v_1, \dots, v_{n-1}$ such that

$$AV = [A\mathbf{1}_n \; Av_1 \; \cdots \; Av_{n-1}] = V \begin{bmatrix} \alpha & \mathbf{0}_{1\times(n-1)} \\ \mathbf{0}_{n-1} & A_1 \end{bmatrix},$$

where $V = [\mathbf{1}_n \; v_1 \; \cdots \; v_{n-1}] \in \mathbb{F}_p^{n\times n}$ is nonsingular in $\mathbb{F}_p$, and $A_1 \in \mathbb{F}_p^{(n-1)\times(n-1)}$ is a nilpotent matrix. For any initial state $x(0) \in \mathbb{F}_p^n$,

$$\begin{aligned} x(n-1) &= A^{n-1}x(0) \\ &= V \begin{bmatrix} \alpha^{n-1} & \mathbf{0}_{1\times(n-1)} \\ \mathbf{0}_{n-1} & \mathbf{0}_{(n-1)\times(n-1)} \end{bmatrix} V^{-1}x(0) \\ &= (\alpha^{n-1} w_1 x(0)) \cdot \mathbf{1}_n \in \Omega, \end{aligned}$$

where w_1 is the first row of V^{-1}. Consequently, synchronization of network (2) over $\mathbb{F}_p$ is achieved. ∎

Example 4 *Consider the network in Example 1. The characteristic polynomial of A is $P_A(\lambda) = \lambda^2(\lambda - 4)$. Therefore, by Theorem 3, the network in Example 1 achieves synchronization.*

From the proof of Theorem 3, synchronization can be achieved in finite time $n-1$ and the synchronization value of network (2) over $\mathbb{F}_p$ is dependent on the initial state value and the first row of V^{-1}. Note that $P_A(\lambda) = \lambda^{n-1}(\lambda - \alpha)$ has n roots in $\mathbb{F}_p$. By algebraic theory, matrix A can be transformed to a Jordan canonical form by a similarity transformation. The convergence time indeed relies on the largest size of the Jordan blocks of A. It can be seen from the following result that for a synchronized network over finite fields, any initial state can reach a periodic behavior in finite time less than n and the periodic behaviors, i.e., the cycles, can be determined by the network matrix and the initial state.

Theorem 4 *Consider network (2) over $\mathbb{F}_p$. Assume that $A\mathbf{1}_n = \alpha \mathbf{1}_n$, where $\alpha \neq 0$ and network (2) over $\mathbb{F}_p$ achieves synchronization. Let $N < n$ be the dimension of the largest Jordan block associated with the eigenvalue 0 and $\eta \in \mathbb{F}_p^n$ be the left eigenvector corresponding to the eigenvalue α satsfying $\eta^T \mathbf{1}_n = 1$. Then for any initial value $x(0) \in \mathbb{F}_p^n$ and any $t \geq N$, $x(t)$ is $\mathbf{0}_n$ or in the set $\{\eta^T x(0)\mathbf{1}_n, \eta^T x(0)\alpha\mathbf{1}_n, \dots, \eta^T x(0)\alpha^{s-1}\mathbf{1}_n\}$, whose elements constitute a cycle $\eta^T x(0)\mathbf{1}_n \to \eta^T x(0)\alpha\mathbf{1}_n \to \cdots \to \eta^T x(0)\alpha^{s-1}\mathbf{1}_n \to \eta^T x(0)\mathbf{1}_n$ in the transition graph $\mathscr{G}_A$, where s is the order of α modulo p. In addition, if the ith entry of η is nonzero, then there are directed paths from agent i to all the other agents.*

Proof. If network (2) over $\mathbb{F}_p$ achieves synchronization, then A can be transformed into a Jordan canonical form J_A as $J_A = V^{-1}AV$, where the nonsingular matrix V can be selected such that the first column of V is $\mathbf{1}_n$ and the first row of V^{-1} is η^T. After N iterations,

$$\begin{aligned} x(N) &= A^N x(0) \\ &= V \begin{bmatrix} \alpha^N & \mathbf{0}_{1\times(n-1)} \\ \mathbf{0}_{n-1} & \mathbf{0}_{(n-1)\times(n-1)} \end{bmatrix} V^{-1}x(0) \\ &= (\eta^T x(0)\alpha^N) \cdot \mathbf{1}_n. \end{aligned}$$

If $\eta^T x(0) \neq 0$, then the state at time N is one vertex in the cycle $\eta^T x(0)\mathbf{1}_n \to \eta^T x(0)\alpha\mathbf{1}_n \to \cdots \to \eta^T x(0)\alpha^{s-1}\mathbf{1}_n \to \eta^T x(0)\mathbf{1}_n$. Otherwise, the state at time N is $\mathbf{0}_n$.

The proof of the final statement is the same as that in Theorem 4.4 in Pasqualetti, Borra & Bullo (2014). ∎

Remark 6 *For network (2) over $\mathbb{F}_p$, one can construct a special network matrix A to achieve synchronization. Specifically, choose A as $A = [v^T, v^T, \dots, v^T]^T$ where v is a row vector, that is, all the rows of A are the same, then network (2) over $\mathbb{F}_p$ achieves synchronization.*

Remark 7 *The results can be extended to high dimensional case. If the state $x_i(t)$ of agent i is not a scalar in $\mathbb{F}_p$ but a* *vector in $\mathbb{F}_p^m$, then network (2) should be modified as*

$$x(t+1) = (A \otimes I_m)x(t), \qquad (6)$$

where $x(t) \in \mathbb{F}_p^{nm}$ and "$\otimes$" is the Kronecker product operator. If synchronization of this network over $\mathbb{F}_p$ is achieved, the trajectories of (6) will enter into the set $\{\mathbf{1}_n \otimes v | v \in \mathbb{F}_p^m\}$ after a finite time. Then either A is a nilpotent matrix or has the same nonzero row sums. All the obtained results in this paper hence can be extended to this high dimensional case.

4 Conclusion

In this paper, the synchronization problem for networks over finite fields was first proposed and investigated by graph theory. Necessary and sufficient conditions were derived for achieving synchronization of networks over finite fields. Our obtained synchronization results outperform the consensus results for networks over finite fields in Pasqualetti, Borra & Bullo (2014) since synchronization include consensus as a special case in this paper. The research topics such as synchronization of switched or delayed networks over finite fields are our further study interests.

References

Burton, D. M. (2006). *Elementary number theory*, Tata McGraw-Hill Education.

Fagiolini, A. & Bicchi, A. (2013). On the robust synthesis of logical consensus algorithms for distributed intrusion detection. *Automatica*, *49*(8), 2339–2350.

Feng, Z., Hu, G. & Wen, G. (2016). Distributed consensus tracking for multi-agent systems under two types of attacks. *International Journal of Robust and Nonlinear Control*, *26*(5), 896–918.

Feng, Z., Wen, G. & Hu, G. (2017). Distributed secure coordinated control for multiagent systems under strategic attacks. *IEEE Transactions on Cybernetics*, *47*(5), 1273–1284.

Garcia, E., Cao, Y., Casbeer, D. W. et al. (2017). Periodic event-triggered synchronization of linear multi-agent systems with communication delays. *IEEE Transactions on Automatic Control*, *62*(1), 366–371.

Hernández Toledo, R. A. (2005). Linear finite dynamical systems. *Communications in Algebra*, *33*(9), 2977–2989.

Hong, Y. & Scaglione, A. (2005). A scalable synchronization protocol for large scale sensor networks and its applications. *IEEE Journal on Selected Areas in Communications*, *23*(5), 1085–1099.

Kashyap, A., Başar, T. & Srikant, R. (2007). Quantized consensus. *Automatica*, *43*(7), 1192–1203.

LeBlanc, H. J. & Koutsoukos, X. (2018). Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multi-agent systems. *IEEE Transactions on Control of Network Systems*, *5*(3), 1219–1231.

Li, H., Zhao, G. & Guo, P. (2018). *Analysis and control of finite-valued systems*. CRC Press.

Li, W., Liu, L. & Feng, G. (2018). Distributed output-feedback tracking of multiple nonlinear systems with unmeasurable states. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, doi: 10.1109/TSMC.2018.2875453.

Li, X., Chen, M. Z. Q., Su, H. & Li, C. (2016). Consensus networks with switching topology and time-delays over finite fields. *Automatica*, *68*, 39–43.

Li, X., Su, H. & Chen, M. Z. Q. (2016). Consensus networks with time-delays over finite fields. *International Journal of Control*, *89*(5), 1000–1008.

Li, Y., Li, H., Ding, X. & Zhao, G. (2019). Leader-follower consensus of multiagent systems with time delays over finite fields. *IEEE Transactions on Cybernetics*, *49*(8), 3203–3208.

Lidl, R. & Niederreiter, H. (1997). *Finite fields*. Vol. 20, Cambridge University Press.

Liu, Z., Zhang, M., Saberi, A. & Stoorvogel, A. A. (2018). State synchronization of multi-agent systems via static or adaptive nonlinear dynamic protocols. *Automatica*, *95*, 316–327.

Liuzza, D., Dimarogonas, D. V., Di Bernardo, M. & Johansson, K. H. (2016). Distributed model based event-triggered control for synchronization of multi-agent systems. *Automatica*, *73*, 1–7.

Meng, M., Liu, L. & Feng, G. (2018). Output consensus for heterogeneous multiagent systems with Markovian switching network topologies. *International Journal of Robust and Nonlinear Control*, *28*(3), 1049–1061.

Moghadam, R., Mustafa, A., Modares, H. & Başar, T. (2018). Resilient output synchronization of heterogeneous multi-agent systems under cyber-physical attacks. *arXiv preprint arXiv:1807.02856*.

Nuno, E., Ortega, R., Basanez, L. & Hill, D. (2011). Synchronization of networks of nonidentical Euler-Lagrange systems with uncertain parameters and communication delays. *IEEE Transactions on Automatic Control*, *56*(4), 935–941.

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

Pasqualetti, F., Borra, D. & Bullo, F. (2014). Consensus networks over finite fields. *Automatica*, *50*(2), 349–358.

Proskurnikov, A. V. (2013). Average consensus in networks with nonlinearly delayed couplings and switching topology. *Automatica*, *49*(9), 2928–2932.

Rahbari-Asr, N., Ojha, U., Zhang, Z. & Chow, M. Y. (2014). Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid. *IEEE Transactions on Smart Grid*, *5*(6), 2836–2845.

Ren, W., Beard, R. W. & Atkins, E. M. (2007). Information consensus in multivehicle cooperative control. *IEEE Control Systems Magazine*, *2*(27), 71–82.

Sundaram, S. & Hadjicostis, C. N. (2013). 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.

Wang, X., Zhu, J. & Feng, J. (2019). A new characteristic of switching topology and synchronization of linear multi-agent systems. *IEEE Transactions on Automatic Control*, *64*(7), 2697–2711.

Xu, X. & Hong, Y. (2014). Leader-following consensus of multi-agent systems over finite fields. in *Proceedings of the 53rd Annual Conference on Decision and Control (CDC)*, IEEE, pp. 2999–3004.