On persistent excitations for the identification of switched linear dynamical systems over finite fields

Gilles Millérioux, Jamal Daafouz

On persistent excitations for the identification of switched linear dynamical systems over finite fields

Gilles Millérioux [a] Jamal Daafouz [b]

[a] *Research Center for Automatic Control of Nancy, University of Lorraine*
Email: {gilles.millerioux}@univ-lorraine.fr

[b] *Research Center for Automatic Control of Nancy, University of Lorraine*
Email: {jamal.daafouz}@univ-lorraine.fr

Abstract

This paper discusses the issue of the Persistent Excitation (PE) conditions in the context of identification for dynamical systems defined over a finite field. The work is motivated by the fact that the asymptotical property of the PE conditions for dynamical systems defined over the field of real numbers is no longer valid in the case of systems defined over finite fields. The special class of switched linear discrete-time systems for which the mode is assumed to be unknown is considered. A necessary and sufficient condition that provides the minimum amount of data required for the identification is first proposed. Next, a necessary condition is derived that gives the structural condition the system must satisfy, regardless of the availability of data. Finally, some computational aspects are discussed and examples are given to illustrate the validity of the proposed results.

Key words: Identification, switched discrete-time systems, finite fields

Discrete Dynamical Systems (DDSs), whereby both time and state space are discrete, are encountered in various practical applications ranging from communication networks to biological systems. These systems, with a countable number of states, are known to be appropriate models in computer science for specification, verification and resource allocation problems on software and hardware systems [1–3]. Typically, manufacturing systems, communication networks, traffic networks, transportation systems and logistic systems can be reasonably modelled under a discrete dynamical framework. In addition, DDSs can be employed in life sciences to model population growth (humans, genes, molecules, neurons). In such areas, discrete models are usually a discrete abstraction of continuous dynamics. This is typically the case in immunology and virology [4], and in applications in biological networks [5–8]. One of the important areas where models over finite fields find its importance is in applications like secure communication and cryptography. Here, DDSs defined over finite fields are used to cipher and decipher data that are intrinsically of a discrete nature. Ciphers can take the form of cellular automata being either autonomous (see [9] for a pioneering work on the topic) or non-autonomous [10].

There exists a variety of formal models to describe DDSs. A detailed classification of DDSs is given in [11] whereby a distinction between the various tools employed for their representation is highlighted; namely graphical tools (state transition diagrams or finite-automata, Petri net, Grafcet, state charts, ladder logic diagrams), algebraic tools (Boolean algebra, algebraic expressions over state space, max-plus algebra) and formal languages. It is also important to note that any one of these representations can be mapped to another. In effect, mappings between finite state automata, Boolean systems and Grafcets to systems described by polynomial expressions over the Galois field are detailed in [12–14].

⋆ Corresponding author G. Millérioux

Apart from modeling, control issues have also been addressed for discrete systems in the literature. The issues of controllability, reachability and state feedback control have been investigated using different approaches such as the theory of polynomial dynamical systems [15], graph theory [16,17], max-plus algebra [18,19], finite field theory [14,20], discrete abstraction and state transition graphs [5], linear modular systems [21] to name a few. Observability for DDSs has also been the subject of a number of research works. For instance, one can refer to the interesting work in [22] which deals with Boolean networks or to [20] where the observability issue is treated for finite multi-agent systems.

Identification plays a centrol role for modeling purposes. An important property in the context of identification is identifiability. Identifiability is related to the notion of uniqueness of solution. Such a notion is important since the estimation of the parameters of a model, with a prescribed structure and based on experimental data, can lead to several solutions. Hence, before proceeding with identification, it is necessary to check whether uniqueness of solution is guaranteed. Uniqueness of solution depends both on the *a priori* structure of the model and on the richness of the data, known as Persistent Excitation (PE) conditions. An exhaustive list of papers dealing with identifiability can be found in [23,24]. However, none of these papers addresses the problem of identifiability for DDSs whereby identifiability may still play a central role and the values of the model parameters may capture some important physical meanings. As mentioned before, cryptography is one of the areas where identification can be applied under a DDS framework. In this context, the parameters of the dynamical system are expected to act as the secret key. Hence, identification can be viewed as an attack which is generally referred to as an algebraic attack. In this case, uniqueness of the solution is a necessary condition for security. Indeed, the larger the key space, the weaker the probability of recovering the secret key by means of an exhaustive search.

Beside discrete dynamical systems, Switched Dynamical Systems (SDSs) are valuable models regardless of whether we consider systems defined over the field of real numbers or over finite fields. Recall that a switch is an event which entails a change in the dynamics of the system. For instance, in circuit theory, that may correspond to a switched capacitor in a digital filter or an electronic switch in a power converter. For an interesting work on finite fields in the context of circuit theory and their applications, the reader may refer to the book [25]. On the other hand, switches may also reflect changes of modes of operation in a plant [19]. More generally, switches may correspond to any transition rule that determines the mode of the system. The mode can be an external event or can depend on the input and/or the state of the system. This is precisely the case of cellular automata [26]. Indeed, a cellular automaton is a discrete dynamical system that consists of an arrangement of basic components, called cells, together with a transition rule based on the states of neighboring cells.

This paper aim to provide a contribution toward the identification of switched dynamical systems over finite fields and to the underlying notion of identifiability. We investigate the case when the discrete mode of the switching rule is not accessible. By being not accessible, it is meant that, for an input-output pair of the data set used for the identification, the corresponding mode is unknown. The purpose of the paper is two-fold: i) to provide a procedure for identifying the parameters of a switched linear discrete system and ii) to reconsider the PE conditions in such a case. Indeed, the PE conditions deserve a special investigation over finite fields because they can no longer be stated similarly to the case of the field of real numbers. The main reason lies in that the PE conditions in the field of real numbers are based on an underlying asymptotic property that does not hold over finite fields. In this regards, two conditions are established. First, we establish a necessary and sufficient condition on the minimum amount of data set required for the identification. Secondly, we establish a necessary condition that gives the system's structural requirement (given the underlying finite field); involving the dimension and the number of modes of the system.

This paper is organized as follows. In Section 1, a background on algebra over finite fields is first recalled. Next, the general principle of the identification procedure for switched linear systems and the associated PE conditions are provided. In Section 2, a structural condition that the dynamical system must fulfill in order to meet the PE conditions is proposed. Finally, in Section 3, computational issues regarding the operations required for the identification over finite fields are addressed. Two simple examples are given to illustrate the approach and to highlight the uniqueness of solution issue.

1 Preliminaries

1.1 Algebra over finite fields - definitions

In this section, we recall some basic and classical definitions that are employed throughout the paper.

Commutative ring:
A commutative ring R is a set of elements and two operations, $+$ and $\cdot$, that are both commutative, associative, distributive and closed in R. Operations $+$ and $\cdot$ have identity elements 0 and 1 respectively. For every element $a \in R$, there exists an element $b \in R$ such that $a + b = 0$, i.e. $+$ has an inverse.

Field:
A field $\mathbb{F}$ is a commutative ring where every element except 0 has a multiplicative inverse, i.e. for every element $a \in \mathbb{F}\backslash\{0\}$, there exists an element $\bar{a} \in \mathbb{F}\backslash\{0\}$ such that $a \cdot \bar{a} = 1$.

Finite field:
A finite field is a field that contains a finite number of elements, which is also referred to as the order of the field. A field of order p will be denoted with $\mathbb{F}_p$.

In this paper, the finite field $\mathbb{F}_p$ under consideration will be the set $\{0, 1, \cdots, p-1\}$ together with the addition and the multiplication modulo p, with p being a prime number.

Polynomial ring:
A polynomial ring denoted by $\mathbb{F}_p[z]$ or $\mathbb{F}_p[z^{(1)}, \ldots, z^{(i)}, \ldots, z^{(n)}]$ is a ring whose elements are polynomials. The indeterminates are the vector components $z^{(i)}$ and the coefficients are in $\mathbb{F}_p$.

1.2 Switched systems over $\mathbb{F}_p$

We consider the switched linear dynamical system:

$$\begin{cases} x_{k+1} &= A_{\sigma(k)} x_k + B_{\sigma(k)} u_k \\ y_k &= C_{\sigma(k)} x_k + D_{\sigma(k)} u_k \end{cases} \tag{1}$$

where $u_k \in \mathbb{F}_p$, $y_k \in \mathbb{F}_p$ and $x_k \in \mathbb{F}_p^n$. The switching function σ

$$\sigma : k \in \mathbb{N} \mapsto j = \sigma(k) \in \{1, \ldots, J\}$$

is arbitrary with J being the number of modes. In other words, at a specific discrete time k, the index j corresponds to the mode of the system given by the switching function σ. No specific dwell time is imposed. The terminology 'dwell time' is used here in accordance with the definition given in [27] for the discrete-time case. Alternatively, the terminology 'dwell iteration' could be used instead. All the matrices, namely $A_{\sigma(k)} \in \mathbb{F}_p^{n\times n}$, $B_{\sigma(k)} \in \mathbb{F}_p^{n\times 1}$, $C_{\sigma(k)} \in \mathbb{F}_p^{1\times n}$ and $D_{\sigma(k)} \in \mathbb{F}_p$ belong to the finite sets $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ respectively.

A sequence of modes over the interval of time $[k_1, k_2]$ is a sequence of $k_2 - k_1 + 1$ integers in the set $\{1, \ldots, J\}$. An admissible sequence of modes is a $(k_2 - k_1 + 1)$-tuple of integers $(i_1, \ldots, i_{k_2-k_1+1})$ which corresponds to a realization $(\sigma(k_1), \ldots, \sigma(k_2))$. The maximum number of admissible sequences is $N = J^{k_2-k_1+1}$. In what follows, the N sequences of modes will be simply denoted by $\sigma_1, \ldots, \sigma_N$. We assume that it is possible to derive an equivalent input/output (I/O) model for the above system. The reader may refer to [28][29] for a detailed explanation of this I/O equivalence problem. In particular, it is shown in [29] that at least all observable systems admit an equivalent I/O model. Furthermore, for $s = 1, \ldots, N$, the I/O model assigned to the state space form (1) can be rewritten, for any discrete-time k, as

$$y_k = \sum_{j=1}^{K_1} a_j(\sigma_s) y_{k-j} + \sum_{j=0}^{K_2} c_j(\sigma_s) u_{k-j} \tag{2}$$

where $a_j(\sigma_s)$ and $c_j(\sigma_s)$ are coefficients depending on the entries of the matrices $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ of (1). The quantities K_1 and K_2 correspond to the maximum number of monomials involving the

outputs and the inputs taken over all the submodels respectively. The coefficients $a_j(\sigma_s)$ and $c_j(\sigma_s)$ of the I/O model (2) can be expressed in terms of the matrices of the state space model (1) by solving a set of linear equations. To this end, the reader may refer to [30] for the case when the system (1) is flat (see [31,32] for general notions on flatness) or to [29] for the general case. In the sequel, we set $K = K_1 + K_2$.

Proposition 1 *The maximum number of input/output relations, $N = N_{I/O}$, regardless of the number J of modes, is finite and equal to $N_{I/O} = p^{K+1}$.*

Proof 1 *The proof is a direct consequence of the fact that i) the input/output relation (2) involves $K+1$ coefficients and ii) each of the coefficient takes its value in the set $\mathbb{F}_p$, which is of finite cardinality p.*

If σ_s is accessible, then the corresponding sequence of modes $\sigma(k), \sigma(k+1), \ldots$ over the horizon $[k, k+max(K_1, K_2)]$ is known. Hence, for every $s \in [1, N]$, an input-output pair of the data set can be assigned to a sequence σ_s. As a result, the identification is easy since for every σ_s ($s \in [1, N]$), the parameters $c_j(\sigma_s)$ and $a_j(\sigma_s)$ appear in a linear fashion in the I/O relation (2). Indeed, for a given sequence of modes σ_s, the identification can be performed by iterating the relation (2) until a set of linear independent equations is obtained and which can then be solved.

In this work, the problem under consideration corresponds to the case where σ_s is not accessible. In such a case, it is impossible to assign the I/O data with the sequence of modes σ_s. The identification procedure employed here is inspired from that suggested in [33] for ARX models over the field of real numbers. Since this procedure constitutes a prerequisite for the main result of the present paper, its main steps are recalled for the sake of clarity.

Each I/O relation (2) can be rewritten, for $s = 1, \ldots, N$, as

$$z_k^T b_s = 0 \tag{3}$$

with

$$z_k = [y_k, \cdots, y_{k-K_1}, u_k, \cdots, u_{k-K_2}]^T \in \mathbb{F}_p^{K+2}$$
$$b_s = [1, -a_1(\sigma_s), \ldots, -a_{K_1}(\sigma_s), -c_0(\sigma_s), \ldots, -c_{K_2}(\sigma_s)]^T \in \mathbb{F}_p^{K+2}$$

Here, z_k is the *regressor vector* while b_s is the *parameter vector* corresponding to the mode sequence σ_s.

Remark 1 *The size of the regressor and of the parameter vector can be clearly reduced if some of the coefficients $a_j(\sigma_s)$ and $c_j(\sigma_s)$ are known or are zero. Indeed, in such a case, the coefficients that are always zero are not incorporated into b_s.*

We define N hyperplanes S_s, $s = 1 \ldots, N$ as

$$S_s = \{z_k : z_k^T b_s = 0\}$$

1.3 Identification procedure and the PE conditions

The following equation holds regardless of the switching sequences

$$p_N(z_k) = \prod_{s=1}^{N} (z_k^T b_s) = \nu_N(z_k)^T h_N = 0 \tag{4}$$

where $h_N \in \mathbb{F}^{M_N}$ is the vector whose components are the coefficient of p_N and $\nu_N : z_k \in \mathbb{F}_p^{K+2} \mapsto \xi_k \in \mathbb{F}_p^{M_N}$ is a map of degree N, the components of ξ_k corresponding to all the M_N monomials (product of the components $z_k^{(i)}$ of z_k) sorted in the degree-lexicographic order [1]. By definition, the map ν_N is a so-called *Veronese map* and the quantity M_N is given by

$$M_N(K) = \frac{(N+K+1)!}{N!(K+1)!} \tag{5}$$

[1] A *lexicographic order* is a ranking according to the names of the variables and their iterates such that:

In the sequel, $M_N(K)$ will be sometimes simply written as M_N when no possible confusion can arise.

Remark 2 *The first component $h_N^{(1)}$ of h_N is equal to 1.*

In [33], the polynomial p_N is referred to as the *Hybrid Decoupling Constraint Polynomial* while the equality (4) as the *Hybrid Decoupling Constraint* equation. It must be stressed that the constraint (4) is still valid in the context of this present study. Indeed, since the multiplication is closed in the ring $\mathbb{F}_p[z]$, the product $p_N(z_k)$ is also in $\mathbb{F}_p[z]$.

For the identification of the parameters b_s in (3), it is first required to compute the coefficients h_N of (4).

Computation of h_N
Let $\mathcal{L}_N$ denote the embedded data matrix involving N' mapped regressor vectors z_k through ν_N

$$\mathcal{L}_N = \begin{bmatrix} \nu_N(z_{k_1}) \\ \nu_N(z_{k_2}) \\ ... \\ \nu_N(z_{k_{N'}}) \end{bmatrix}^T \in \mathbb{F}_p^{N' \times M_N} \tag{6}$$

The following relation applies:

$$\mathcal{L}_N h_N = \mathbf{0} \tag{7}$$

The following proposition gives a necessary and sufficient condition that must be fulfilled by the regressors. It allows to assess the minimum amount of data that is required for the identification to guarantee uniqueness of solutions.

Proposition 2 *The solutions space of (7) is of dimension one and the uniqueness of h_N is ensured if and only if the integer N' is large enough so that the $\nu_N(z_{k_i})$ $(i = 1, \ldots, N')$ satisfies*

$$rank(\mathcal{L}_N) = M_N - 1 \tag{8}$$

Proof 2 *The rank condition (8) guarantees that the $\nu_N(z_{k_i})$ $(i = 1, \ldots, N')$ span a $M_N - 1$ dimensional vector space. Since $\mathcal{L}_N$ is of dimension $N' \times M_N$, the solution of (7) is one-dimensional. In addition, h_N is unique according to Remark 2 and can be calculated by*

$$h_N \in Ker(\mathcal{L}_N) \text{ such that } h_N^{(1)} = 1 \tag{9}$$

The lower bound of N' is clearly $M_N - 1$. Recall that over $\mathbb{R}$, the assumption that the mapped regressor vectors $\nu_N(z_{k_i})$ are *sufficiently exciting* is known as the Persistent Excitation (PE) conditions [34]. Over a finite field such as $\mathbb{F}_p$, the number of possible regressors z_{k_i} is finite, and thus, the definition used over $\mathbb{R}$ no longer holds. The PE conditions are expressed in terms of the rank condition (8).

Computation of b_s
Let us first recall the following definition:

Definition 1 *[35] A derivative D on the field $\mathbb{F}_p$ is a mapping $D : \mathbb{F}_p \mapsto \mathbb{F}_p$ which is linear and satisfies the ordinary rule for derivatives, i.e., for every element x, y in $\mathbb{F}_p$, $D(x + y) = D(x) + D(y)$ and $D(x \cdot y) = xD(y) + yD(x)$.*

As a result, the derivative $Dp_N(z_k)$ of $p_N(z_k)$ in (4) is also in the polynomial ring $\mathbb{F}_p[z]$ and is given by

$$Dp_N(z_k) = \frac{\partial p_N(z_k)}{\partial z_k} = \frac{\partial}{\partial z_k} \prod_{s=1}^{N} ({z_k}^T b_s) = \sum_{s=1}^{N} b_s \prod_{l \neq s}^{N} ({z_k}^T b_l). \tag{10}$$

- $z_k^{(i)} < z_{k+l}^{(i)}$, $\forall l \in \mathbb{N}$,
- $z_m^{(i)} < z_l^{(j)} \Rightarrow z_{m+t}^{(i)} < z_{l+t}^{(j)}$, $\forall m \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall t \in \mathbb{N}$,
- $z_k^{(i)} < z_k^{(j)} \Rightarrow (z_k^{(i)})^\alpha < (z_k^{(j)})^\beta$, $\forall \alpha \in \mathbb{N}$, $\forall \beta \in \mathbb{N}$

We rewrite (10) as

$$Dp_N(z_k) = b_s \prod_{l \neq s}^{N} ({z_k}^T b_l) + \sum_{i \neq s}^{N} b_i \prod_{j \neq i}^{N} ({z_k}^T b_j). \tag{11}$$

Now, consider an arbitrary vector $w_s \in \mathbb{F}_p^{K+2}$ such that $w_s^T b_s = 0$. Replacing w_s $(s = 1, \ldots, N)$ into (11) yields

$$Dp_N(w_s) = b_s \prod_{l \neq s}^{N} (w_s^T b_l) \tag{12}$$

One could be concerned by the fact that the quantity b_s is defined up to the scalar $\prod_{l \neq s}^{N} (w_s^T b_l)$, which is actually unknown. Indeed, its computation would require the knowledge of all vectors b_s, $l \neq s$. However, since $Dp_N(w_s)$ is known and the first component of b_s is equal to 1, the true parameter vector b_s is obtained by merely normalizing $Dp_N(w_s)$. Hence, whenever the solution h_N is guaranteed to be one-dimensional, its uniqueness, as well as the uniqueness of the b_s, is also guaranteed.

2 Structural conditions

In this section, a necessary condition is established. It gives a structural condition that the system needs to satisfy in order for the kernel h_N to be one-dimensional, regardless of whether the data is available or not. Note that the system can be characterized by the triplet (p, K, N). Consequently, we can state the following proposition:

Proposition 3 *In order for the kernel h_N to be one-dimensional, it is necessary that the triplet (p, K, N) satisfies*

$$p^{(K+1)} \geq M_N(K) - 1 \tag{13}$$

Proof 3 *First, let note that the maximum number $N' = N'_{max}$ of regressors z_{k_i} that (1) can generate, regardless of the number J of modes, is $N'_{max} = p^{K+1}$.*
Indeed, the number of components of the regressor vector z_k is $K+2$. On the other hand, regarding (2), the component y_k is linearly congruent to the other ones that are $y_{k-1}, \ldots, y_{k-K_1}, u_k, \ldots, u_{k-K_2}$. These $K+1$ components take value in the set $\mathbb{F}_p$ which is of finite cardinality p.

Moreover, the Veronese map in (4)

$$\nu_N : z_k \in \mathbb{F}_p^{K+2} \mapsto \xi_k \in \mathbb{F}_p^{M_N}$$

is surjective over the finite field $\mathbb{F}_p$. Thus, the cardinality of the sets $\{z_k\}$ and $\{\xi_k\}$ satisfies:

$$card\,(\{\xi_k\}) \leq card\,(\{z_k\}) \leq N'_{max} = p^{(K+1)}$$

It follows that

$$rank(\mathcal{L}_N) \leq N'_{max} = p^{(K+1)} \tag{14}$$

Finally, by considering the relations (8) and (14), we obtain the condition of the proposition and which completes the proof of the latter.

The following proposition allows to assess the influence of the triplet (p, K, N) on the uniqueness of the kernel.

Proposition 4 *For every pair (p, K_c) with $p \geq 2$, there exists an integer $N \in [1, N_{I/O}]$ such that*

$$M_N(K) - 1 \leq N'_{max} = p^{(K+1)}$$

for $K \geq K_c$

Proof 4 *First, let us recall the expression (5) of $M_N(K)$:*

$$M_N(K) = \frac{(N + K + 1)!}{N!(K + 1)!}$$

On one hand, since $M_1(K) - 1 = K + 1$, it is clear that, for all $p \geq 2$ and for all K

$$p^{(K+1)} > M_1(K) - 1 \tag{15}$$

On the other hand, for all $p \geq 2$ and for all K

$$p^{(K+1)} < M_{N_{I/O}}(K) - 1 \tag{16}$$

Next, for all $p \geq 2$ and all $l \in \{2, \ldots, K+1\}$, we have

$$p^{K+1} + l > l$$

Hence,

$$\prod_{i=2}^{K+1} (p^{K+1} + i) > (K+1)!$$

Multiplying both sides by $(p^{(K+1)} + 1)!$ yields

$$\begin{aligned} &(p^{(K+1)} + 1)! \textstyle\prod_{i=2}^{K+1} (p^{K+1} + i) > (p^{(K+1)} + 1)!(K+1)! \\ &\Leftrightarrow (p^{(K+1)} + K + 1)! > (p^{(K+1)} + 1)!(K+1)! \end{aligned}$$

Dividing both sides by $(p^{(K+1)})!(K+1)!$, we get

$$\frac{(p^{(K+1)} + K + 1)!}{(p^{(K+1)})!(K+1)!} - 1 > p^{(K+1)}$$

Now, from (5) and taking into account that $N_{I/O} = p^{K+1}$, the following equality holds:

$$M_{N_{I/O}}(K) = \frac{(p^{(K+1)} + K + 1)!}{(p^{(K+1)})!(K+1)!}$$

which proves (16).

Finally, it is easy to see that the functions $K \to p^{K+1}$ and $K \to M_N(K) - 1$, for any N, are monotonically increasing with respect to K. As a result, for all pairs (p, K) with $p \geq 2$, there exists an integer $N \in [1, N_{I/O}]$ so that the functions $K \to p^{K+1}$ and $K \to M_N(K) - 1$ intersect each other. Then, for all pairs (p, K_c) with $p \geq 2$, there exists an integer N so that $p^{(K+1)} > M_N(K) - 1$ for $K \geq K_c$. This completes the proof of Proposition 4.

In other words, Proposition 4 gives, for a given cardinality p of the set $\mathbb{F}_p$ and a prescribed integer K (related to the dimension n of the system), a bound on the number N of I/O relations (related to the number J of modes) so that (13) is satisfied. However, although (13) holds, owing to the dynamics of the system, the number N' of independent regressors z_{k_i} may be lower than the maximum number N'_{max}. Indeed, the trajectory of the state vector does not necessarily visit all the possible states over $\mathbb{F}_p$. Hence, the maximum rank of the embedded data matrix may not attain $M_N(K) - 1$, thereby preventing the uniqueness of h_N. A graphical interpretation of Proposition 4 is illustrated in Fig. 1. For a prescribed p, all the pairs (K, N) with $K > K_c$ for which the curve p^{K+1} is above the curve $M_N(K) - 1$ satisfy (13). Therefore, it turns out that the larger the distance between p^{K+1} and $M_N(K) - 1$, the higher the chance of getting sufficient independent regressors to guarantee uniqueness of the solution.

Remark 3 *It is worth pointing out that the result still holds for dynamical systems with state-transition functions and output functions with polynomial nonlinearities, including Boolean functions. Indeed, for such systems, the I/O relations take the form of a linear combination of monomials, involving the products of inputs and outputs which are generically written as $y_k^{p_0} \cdots y_{k-K_1}^{p_{K_1}} u_k^{r_0} \cdots u_{k-K_2}^{p_{k_2}}$. It is clear that switched linear systems constitute a special case with monomials of degree no greater than 1. Such an I/O relation can be obtained by resorting to standard elimination techniques (for example see the Gröbner basis approach [36]). As a result, equation* (3)*, on which all the remaining reasoning is based, still applies whenever the regressor vector $z_k = [y_k, \cdots, y_{k-K_1}, u_k, \cdots, u_{k-K_2}]^T$ is replaced by the vector whose components are the monomials $y_k^{p_0} \cdots y_{k-K_1}^{p_{K_1}} u_k^{r_0} \cdots u_{k-K_2}^{p_{k_2}}$.*

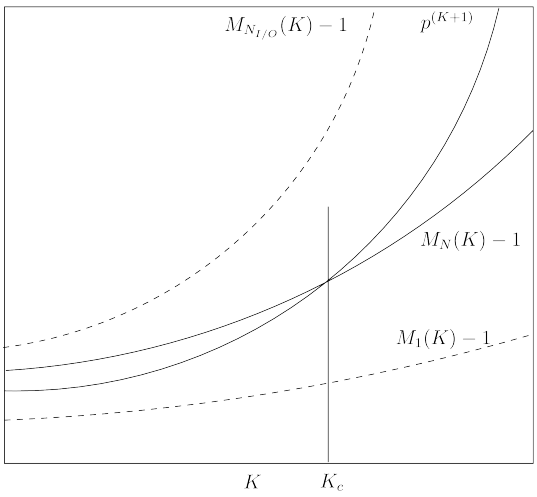

Fig. 1. Graphical interpretation of Proposition 4

3 Practical considerations and examples

3.1 Computation of the kernel

To calculate the kernel in (9), we can resort to a Gaussian elimination over $\mathbb{F}_p$. However, compared with the computation over $\mathbb{R}$, the method must be slightly modified by replacing the division operation by the multiplication with the inverse over the finite field $\mathbb{F}_p$. Among the efficient procedures for inversion over a finite field like $\mathbb{F}_p$, the Extended Euclidean Algorithm [37] is particularly interesting. It is based on the computation of a greatest common divisor.

3.2 Calculating the points w_s

To calculate the N distinct points w_s that lie on the N hyperplanes S_s, the following algebraic procedure can be followed.

Consider a parametrized random line with direction v and base point w_0:

$$\mathcal{D} : \mu v + w_0 \quad \forall \mu \in \mathbb{Z}$$

The line $\mathcal{D}$ intersects with all the hyperplanes at N distinct points under the condition that it is not parallel with any hyperplanes. In other words, the equation of degree N

$$p_N(\mu v + w_0) = 0 \tag{17}$$

admits N distinct integer roots $\{\mu_s\}_{s=1}^{N}$ under the constraint $p_N(v) \neq 0$ (or equivalently $v \notin S_s$). Therefore, the intersection of $\mathcal{D}$ with all of the hyperplanes are given by

$$w_s = \mu_s v + w_0 \quad \forall s \in \{1, .., N\}$$

Since w_s belongs to a finite field, an exhaustive search for the recovery of μ_s could be effective and could act as an alternative to solving (17).

3.3 Examples

The aim of this subsection is to illustrate, with two simple examples, the identification procedure over finite fields and to highlight the influence of the triplets $\{p, N, K\}$ on the uniqueness of the solution.

3.3.1 Example 1

Consider a one-dimensional switched dynamical system over the finite field $\mathbb{F}_{251}$ ($p = 251$) of the form (1) with $A_{\sigma(k)} = q_{\sigma(k)} \in \mathbb{F}_{251}$, $B_{\sigma(k)} = 5$, $C_{\sigma(k)} = 1$, $D_{\sigma(k)} = 0$. The switching function $\sigma(k)$ is assumed to be inaccessible and defined by:

$$\sigma : k \in \mathbb{N} \mapsto \sigma(k) = j \in \{1, 2\}$$

and finally $q_{\sigma(k)} = \{q_1, q_2\} = \{38, 213\}$.

The I/O model is given by:

$$y_k = q_{\sigma(k-1)} y_{k-1} + 5u_{k-1} \tag{18}$$

The two parameter vectors are $b_1 = [1, -q_1, -5]^T$ and $b_2 = [1, -q_2, -5]^T$. Since $213 = -38$ (mod 251) and $246 = -5$ (mod 251), it results that $b_1 = [1, 213, 246]^T$ and $b_2 = [1, 38, 246]^T$. For this example $K = 1$.

The regressor vector is given by $z_k = [y_k, y_{k-1}, u_{k-1}]^T$ and, according to the proof of Proposition 3, the maximum number of regressors is $N'_{max} = p^{K+1} = 251^{1+1} = 63001$. On the other hand, there exist two input/output relations according to the value of $q_{\sigma(k)}$. Hence, $N = 2$.

For $N = 2$ and $K = 1$, we have $M_N(K) - 1 = 5$. Thus, the necessary condition (13) is fulfilled but h_N may be not unique.

Computation of h_N
After applying a sufficiently long input sequence to (1), it turns out that the embedded data matrix $\mathcal{L}_N$ reaches its maximal rank. After a Gaussian elimination, a kernel of dimension one is obtained and, after normalization (see Remark 2), is given as:

$$h_N = [1,\ 0,\ 241,\ 62,\ 0,\ 25]^T$$

Computation of b_s
First, we compute $N = 2$ points w_s so that $w_s^T b_s = 0$. Now, consider a random line $\mathcal{D}$ with a direction $v = [25, 181, 61]^T$ and a base point $w_0 = [42, 155, 208]^T$. Solving (17) gives the solution $\mu_1 = 59$, $\mu_2 = 197$ with two corresponding intersections $w_1 = [11, 41, 42]^T$, $w_2 = [198, 170, 177]^T$.

Finally, the parameter vectors b_s according to (12) are given by:

$$b_1 = [1, 213, 246]^T$$
$$b_2 = [1,\ 38, 246]^T$$

As expected, the correct parameter vectors b_s are obtained. This result can be explained by the fact that not only the necessary condition (13) is fulfilled but also because the number of independent regressor vectors is large enough.

3.3.2 Example 2

Consider a one-dimensional switched dynamical system over the finite field $\mathbb{F}_2$ ($p = 2$) of the form (1) with $A_{\sigma(k)} = q_{\sigma(k)} \in \{0, 1\}$, $B_{\sigma(k)} = C_{\sigma(k)} = 1$ and $D_{\sigma(k)} = 0$. The corresponding I/O model is given by:

$$y_k = q_{\sigma(k-1)} y_{k-1} + u_{k-1}$$

For this example, $K = 1$. The regressor vector is given by $z_k = [y_k, y_{k-1}, u_{k-1}]^T$ and, according to the proof of Proposition 3, the maximum number of regressors is $N'_{max} = p^{K+1} = 2^{1+1} = 4$. Also, there exist two input/output relations according to the value of $q_{\sigma(k-1)}$. Hence, $N = 2$.

For $N = 2$ and $K = 1$, we have $M_N(K) - 1 = 5$. Thus, the necessary condition (13) is not fulfilled. Consequently, it is impossible for the kernel h_N to be one-dimensional. This is explained by the fact that, regardless of the dynamics, the number of independent regressor vectors cannot be large enough.

The embedded data matrix $\mathcal{L}_N$ cannot reach its maximum rank. A Gaussian elimination yields, precisely, four possible vectors h_N for the kernel of $\mathcal{L}_N$:

$$h_N \in (\ [1,1,1,0,0,0]^T, [1,1,0,0,1,1]^T, \\ [1,0,0,1,0,1]^T, [1,0,1,1,1,0]^T\ )$$

For each vector of the kernel h_N, the corresponding parameter vector b_s can be assigned. Only the vector $[1,1,0,0,1,1]^T$ of h_N gives the correct solution for b_s: $b_1 = [1,1,1]^T$ and $b_2 = [1,0,1]^T$.

Remark 4 *The maximum number of regressors is $N'_{max} = p^{K+1} = 2^{1+1} = 4$ but actually, only two independent regressors are obtained. This explains why h_N involves four distinct vectors since $M_N(K) - 2 = 6 - 2 = 4$.*

4 Concluding remarks

In this paper, the persistent excitation conditions that guarantee the uniqueness of the solution for identification problems have been revisited in order to treat dynamical systems defined over finite fields. Special emphasis has been placed on switched linear discrete-time systems. First, a necessary and sufficient condition that provides the minimum amount of data required for the identification has been proposed. Next, a necessary condition that gives the structural constraint the system must satisfy, regardless of the availability of the data, is derived. The necessary condition involves the dimension and the number of modes of the system. Some examples are given to illustrate the validity of the results.

References

[1] B. Caillaud, P. Darondeau, L. Lavagno, and Xiaolan Xie (eds.). *Synthesis and Control of Discrete Event Systems*. Kluwer Academic Press, 2002.

[2] M.C. Zhou and F. Dicesare. *Petri Net Synthesis for Discrete Event Control of Manufacturing Systems*. Springer, 1993.

[3] P.R. Kumarand P; P. Varaiya. *Discrete Event Systems, Manufacturing Systems, and Communication Networks*. Springer Verlag NY, 1995.

[4] E. Delgado-Eckert. Reverse engineering time discrete finite dynamical systems: A feasible undertaking? *PLoS ONE*, 4(3), 03 2009.

[5] G. Batt, H. de Jong, M. Page, and J. Geiselmann. Symbolic reachability analysis of genetic regulatory networks using discrete abstractions. *Automatica*, 44:982 989, 2008.

[6] R. Laubenbacher, A.S. Jarrah, E. Dimitrova, B. Stigler, and P. Vera-Licona. System identification for discrete polynomial models of gene regulatory networks. In *Proc. of the 15th IFAC Symposium on System Identification*, 2009.

[7] E. Dimitrova, L. Garcia-Puente, F. Hinkelmann, A. Jarrah, R. Laubenbacher, B. S. Stigler, and M. Stillman. Parameter estimation for boolean models of biological networks. *Journal of Theoretical Computer Science*, 412(26):2816–2826, 2011.

[8] B. Stigler. Polynomial dynamical systems in systems biology. In *Modeling and simulation of biological networks*, volume 64 of *Proc. Sympos. Appl. Math.* Amer. Math. Soc., 2007.

[9] S. Wolfram. Cryptography with cellular au- tomata. In *Proc. of Crypto 85*, 1986.

[10] S. Tripathy1 and S. Nandi. Lcase: Lightweight cellular automata-based symmetric-key encryption. *International Journal of Network Security*, 8(2):43–252, 2009.

[11] B. Hrúz and M. Zhou. *Modeling and Control of Discrete-event Dynamic Systems*. Springer, 2007.

[12] R. Germundsson. *Symbolic Systems - Theory, Computation and Applications*. PhD thesis, Linkoping University, 1995.

[13] J. Gunnarsson. Algebraic methods for discrete event systems - a tutorial. In *Proc. of Workshop on Discrete Event Systems (WODES'96)*, Edinburgh, Scotland, UK, August 1996.

[14] J. Reger. *Linear Systems over Finite Fields - Modeling, Analysis and Synthesis*. PhD thesis, Universitat Erlangen-Nurnberg, 2004.

[15] M. Le Borgne, A. Benveniste, and P. Le Guernic. Dynamical systems over galois fields and deds control problems. In *Proceedings. 30th IEEE Conference on Decision and Control CDC 1991*, Brighton, UK, December 1991.

[16] E. Delgado-Eckert. Boolean monomial control systems. *Mathematical and Computer Modelling of Dynamical Systems: Methods, Tools and Applications in Engineering and Related Sciences*, 15(2):107–137, 2009.

[17] D. Bollman, O. Colón-Reyes, V. A. Ocasio, and E. Orozco. A control theory for boolean monomial dynamical systems. *Discrete Event Dynamic Systems*, 20(1):19–35, March 2010.

[18] B. De Schutter and T. van den Boom. Max-plus algebra and max-plus linear discrete event systems: An introduction. In *Proceedings of the 9th International Workshop on Discrete Event Systems (WODES'08)*, Goteborg, Sweden, May 2008.

[19] S. Van Loenhout, T. Van den Boom, S. Farahani, and B. De Schutter. Model predictive control for stochastic switching max-plus-linear systems. In *Proceedings of the 11th International Workshop on Discrete Event Systems (WODES'2012)*, 2012.

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

[21] E. Delgado-Eckert, J. Reger, and K. Schmidt. *Discrete Time Systems (Editor: M. A. Jordán)*, chapter Discrete Time Systems with Event-Based Dynamics: Recent Developments in Analysis and Synthesis Methods. InTech, 2011.

[22] S. Sundaram and C. N. Hadjicostis. Information dissemination in networks via linear iterative strategies over finite fields. In *Proc. of the 48th IEEE Conference on Decision and Control (CDC'09)*, Shangha, December 2009.

[23] F. Anstett, G. Bloch, G. Millérioux, and L. Denis-Vidal. Identifiability of discrete-time nonlinear systems: the local isomorphism approach. *Automatica*, 44(1):2884–2889, November 2008.

[24] N.D. Evans, H.A.J. Moyse, D. Lowe, D. Briggs, R. Higgins, D. Mitchell, D. Zehnder, and M.J. Chappell. Structural identifiability of surface binding reactions involving heterogeneous analyte: Application to surface plasmon resonance experiments. *Automatica*, 49(1):48 – 57, 2013.

[25] R. Lidl and H. Niederreiter. *Finite fields*. Cambridge University Press, 2008.

[26] J. V. Neumann. *The Theory of Self-Reproducing Automata*. Univ. of Illinois Press, 1966.

[27] J.C. Geromel and P. Colaneri. Stability and stabilization of discrete time switched systems. *International Journal of Control*, 79(7):719–728, 2006.

[28] S. Weiland, A. Lj. Juloski, and B. Vet. On the equivalence of switched affine models and switched ARX models. In *45th IEEE Conf. on Decision and Control*, 2006.

[29] S. Paoletti, A. Garulli, J. Roll, and A. Vicino. A necessary and sufficient condition for input-output realization of switched affine state space models. In *48th IEEE Conf. on Dec. and Control (CDC 2008)*, Cancún, México, December 2008.

[30] P. Vo Tan, G. Millérioux, and J. Daafouz. Left invertibility, flatness and identifiability of switched linear dynamical systems: a framework for cryptographic applications. *International Journal of Control*, 83(1):145–153, january 2010.

[31] M. Fliess, J. Levine, P. Martin, and P. Rouchon. Flatness and defect of non-linear systems: introductory theory and examples. *Int. Jour. of Control*, 61(6):1327–1361, 1995.

[32] G. Millérioux and J. Daafouz. Flatness of switched linear discrete-time systems. *IEEE Trans. on Automatic Control*, 54(3):615–619, March 2009.

[33] Y. Ma and R. Vidal. Identification of deterministic switch arx system via identification of algebraic varieties. In M. Morari and L. Thiele, editors, *In Proc. 8th International Workshop on Hybrid Systems: Computation and Control*, volume 3414, pages 449–465. Springer-Verlag Berlin Heideberg 2005, 2005.

[34] G. C. Goodwin and K. S. Sin. *Adaptive Filtering Prediction and Control*. Dover Publications, Inc., New York, NY, USA, 2009.

[35] S. Lang. *Algebra, Graduate Texts in Mathematics*. Berlin,New York: Springer-Verlag, 2002.

[36] B. Buchberger. Grobner bases: an algorithmic method in polynomial ideal theory. In *Multidimensinal Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems*, pages 184–232. Reidel Publishing Company, 1985.

[37] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.