

A contribution to the identification of switched dynamical systems over finite fields

Phuoc Vo Tan*, G. Millérioux* and Jamal Daafouz*

* Nancy University

Research Center for Automatic Control of Nancy (CRAN UMR CNRS 7039), France

Corresponding author: gilles.millerioux@esstin.uhp-nancy.fr

Abstract—In this paper, we address specific issues related to the problem of parameter identification for switched linear systems over finite fields. Peculiarities related to the consideration of finite fields are pointed out. In particular, one of the main contributions of the paper is the reconsideration of the usual Persistently Exciting conditions. Indeed they are important in that they guarantee unicity in the solution of the identification procedure but they actually do no longer make sense on finite fields. In this paper, we provide alternative conditions. Such an issue has a cryptographic interest since identification amounts to an attack in cryptography, that is a way of recovering the secret key played by the parameters of the dynamical system.

Discrete dynamical systems are mathematical models with finite state space. They are often encountered not only in engineering and computer science but in the life sciences as well. Indeed, they have been used as models of biological systems since the invention of cellular automata by Von Neumann when attempting to model a self-replicating organism in the 1950s. Since then, they have been used increasingly in systems biology to model a variety of biochemical networks. Let us mention for instance molecular networks inside human cells which process external signals and drive cellular metabolism, gene regulatory networks, large-scale epidemiological networks. Discrete dynamical systems are relevant insofar as most often, the experimental data are available with parsimony, causing continuous models such as ordinary differential equations not very suitable and difficult to obtain with accuracy.

On the other hand, hybrid systems have inspired a great deal of research from both control theory and theoretical computer science [1]. They provide a strong theoretical foundation which combines discrete-event and continuous-time systems in a manner that can capture software logic and physical dynamics in a unified modeling framework. The most well-known area of applicability of hybrid systems are naturally modeling, analysis and control design of embedded systems.

Interesting pioneering works jointly involving hybrid dynamical systems and systems described over finite fields have been proposed within the area of computer science in [2]. The authors propose therein a theory which generalizes the notion of discrete-event dynamical systems.

This theory is supported by a programming language called SIGNAL and a mathematical model of relational style. This framework makes it possible to formulate in the same way programming or specification of hybrid dynamical systems as well as control. In [3], the authors further demonstrate the usefulness of classical control theory concepts for the class of dynamical systems over Galois fields.

In this paper, we address the identification for switched linear systems over finite fields. It is inspired from the procedure suggested in [4] for ARX models over the field of real numbers. One of the main contribution of the present paper is the reconsideration of the usual Persistently Exciting (PE) conditions which actually do no longer make sense on finite fields. We provide alternative conditions to guarantee unicity in the solution of the identification procedure for the class of switched linear systems. Batch identification is considered. Furthermore we investigate the case when the discrete mode of the switching rule is not accessible. These two special considerations are in accordance with the underlying engineering application for which identification is central: symmetric cryptography. Indeed, dynamical systems are involved in design of a special class of ciphers called self-synchronizing stream ciphers [5][6]. It has been shown very recently in [7][8][9] that control theoretical concepts together with switched systems could define an interesting framework for the design of such ciphers. In particular, identifiability and identification are central insofar as the parameters of the dynamical system are expected to act as the secret key, the identification can be thereby viewed as an attack called in cryptography algebraic attack. However, if a digital application is sought (streaming, implementation in e.g. FPGA or DSP, ...), the data to be encrypted are either intrinsically digital or digitalized and so lie in a finite set. This being the case, the dynamical systems can no longer be described on the set of real numbers but on finite sets.

The layout of this paper is the following. In Section I, the general principle of the identification procedure for switched linear systems is provided. Background on algebra over finite fields are recalled. In Section II, the usual PE conditions are reconsidered. Alternative conditions to guarantee unicity in the solution of the identification procedure are given. Finally, in Section III, practical issues regarding the operations over

finite fields required within the identification procedure such as computing the kernel of the matrix of regressors or performing a multiplicative inverse, are addressed. Two simple examples are given to illustrate the identification procedure with special emphasis on the unicity problem.

I. GENERAL PRINCIPLE

A. Background on algebra over finite fields

Finite field:

Given any integer a and a positive integer p , we define and denote $a \pmod{p}$ the division of a by p that leaves the remainder between 0 and $p - 1$. We call two integers a and b to be congruent modulo p if $a \pmod{p} = b \pmod{p}$ and we express such a congruence by $a = b \pmod{p}$. We denote \mathbb{F}_p the set $\mathbb{F}_p = \{0, 1, \dots, p - 1\}$, that is the set of remainders in arithmetic modulo p . When p is a prime number, \mathbb{F}_p is a field.

Indeed, \mathbb{F}_p is first of all a ring, that is a set together with two laws of composition (two mappings $\mathbb{F}_p \times \mathbb{F}_p \mapsto \mathbb{F}_p$), namely the addition (denoted $+$) and the multiplication (denoted \cdot or without any symbols) modulo p . The addition is associative and commutative and has a unit element denoted 0 (for every element $x \in \mathbb{F}_p$, the relation $x + 0 = 0 + x = x$ applies) and has an inverse (for every element $x \in \mathbb{F}_p$, there exists an element $y \in \mathbb{F}_p$ such that $x + y = y + x = 0$). The multiplication is associative and has a unit element denoted 1 (for every element $x \in \mathbb{F}_p$, the relation $x \cdot 1 = 1 \cdot x = x$ applies). Besides, distributivity of the addition over the multiplication applies (for all $x, y, z \in \mathbb{F}_p$ one has $(x + y)z = xz + yz$).

Furthermore, \mathbb{F}_p is a division ring that is a ring such that $1 \neq 0$, and such that every non-zero element is invertible (for every element $x \in \mathbb{F}_p$ there exists an element $y \in \mathbb{F}_p$ such that $x \cdot y = y \cdot x = 1$). The existence of an inverse for every non-zero elements is guaranteed by the fact that p is prime.

Finally, \mathbb{F}_p is a field because it is a commutative division ring (that is the multiplication is commutative).

Polynomial ring:

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

All along this paper, the addition and the multiplication are performed modulo p and for shortness, $(\text{mod } p)$ will be omitted.

B. Switched systems over a finite field

We consider the switched linear dynamical system:

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

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

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

is arbitrary, in particular no dwell time is assumed. J is the number of modes. 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 respective finite sets $(A_j)_{1 \leq j \leq J}$, $(B_j)_{1 \leq j \leq J}$, $(C_j)_{1 \leq j \leq J}$ and $(D_j)_{1 \leq j \leq J}$. At a given time k , the index j corresponds to the mode of the system given by the switching function σ . It is worth pointing out that the writing $\sigma(k)$ is abusive and somehow misleading but used for short. Indeed, the dynamical system (1) is a switched system and not a time-varying system.

Let $\{\sigma_1\}_{k+k_1}^{k+k_2}, \dots, \{\sigma_N\}_{k+k_1}^{k+k_2}$ the N possible mode sequences $\{\sigma(k+k_1), \dots, \sigma(k+k_2)\}$ over any interval of time $[k+k_1, k+k_2]$. If all the mode sequences are admissible, one has $N = J^{k_2-k_1+1}$. These mode sequences will be respectively denoted for short $\sigma_1, \dots, \sigma_N$ in the sequel. We assume that it is always possible to derive an equivalent input/output model. The reader may refer to [10] or [11] for a deep consideration of this problem. For $t = 1, \dots, N$, the input/output relation of the state space model (1) can be rewritten, for any discrete-time k , as

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

where the $a_j(\sigma_t)$ s and the $c_j(\sigma_t)$ s are coefficients depending, in different ways according to the sequence σ_t , 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). K_1 and K_2 are the supremum of the number of monomials involving respectively the outputs and the inputs taken over all the submodels. In the further developments, we let $K = K_1 + K_2$.

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

Proof: The proof is an immediate consequence of the two following facts. The input/output relation (2) involves $K + 1$ coefficients. Besides, each of them takes value in the set \mathbb{F}_p which is of finite cardinality p . ■

If σ_t is accessible, since for each σ_t , the parameters $c_j(\sigma_t)$ and $a_j(\sigma_t)$ appear in a linear fashion in the input/output relation (2), the identification is easy. Indeed, for a given mode sequence σ_t , the identification can be performed by iterating the relation (2) until a set of linear independent equations is obtained and can be solved.

The problem under consideration in this paper corresponds to the case when σ_t is not accessible.

Each input/output relation (2) can be rewritten for $t = 1, \dots, N$ as:

$$z_k^T b_t = 0 \quad (3)$$

with

$$z_k = [y_k, \dots, y_{k-K_1}, u_k, \dots, u_{k-K_2}]^T \in \mathbb{F}_p^{K+2}$$

$$b_t = [1, -a_1(\sigma_t), \dots, -a_{K_1}(\sigma_t), -c_0(\sigma_t), \dots, -c_{K_2}(\sigma_t)]^T \in \mathbb{F}_p^{K+2}$$

z_k is the regressor vector while b_t is the parameter vector corresponding to the mode sequence σ_t .

Remark 1: The size of the regressor and parameter vectors can be obviously reduced if some of the coefficients $a_j(\sigma_t)$ s and $c_j(\sigma_t)$ s are known. A special case is when they are zero. In such a situation, K corresponds to the number of unknown coefficients.

We can thereby define N hyperplanes S_t , $t = 1, \dots, N$

$$S_t = \{z_k : z_k^T b_t = 0\}$$

C. Identification procedure

The following equation applies regardless of the switching sequences:

$$p_N(z_k) = \prod_{t=1}^N (z_k^T b_t) = \nu_N(z_k)^T h_N = 0 \quad (4)$$

It is called *Hybrid Decoupling Constraint* equation and p_N is the *Hybrid Decoupling Constraint Polynomial*. Since the multiplication is closed in the ring $\mathbb{F}_p[z_k]$, the product $p_N(z_k)$ is also in $\mathbb{F}_p[z_k]$.

Remark 2: The first component $h_N^{(1)}$ of h_N equals 1

$h_N \in \mathbb{F}^{M_N}$ is the coefficient of the *Hybrid Decoupling Polynomial* and $\nu_N : z_k \in \mathbb{F}_p^{K+2} \mapsto \xi_k \in \mathbb{F}_p^{M_N}$ is a *Veronese 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 order¹. The quantity M_N depends on K and is given by

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

For shortness, $M_N(K)$ will be sometimes merely written M_N in the sequel.

For the identification of the b_t 's in (3), it is first required to compute the coefficients h_N of (4).

Computing h_N

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

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

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

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

The following relation applies:

$$\mathcal{L}_N h_N = 0 \quad (7)$$

If N' is an integer large enough so that the $\nu_N(z_{k_i})$'s ($i = 1, \dots, N'$) can span a $M_N - 1$ dimensional vector space, i.e.

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

then h_N is one-dimensional and according to the Remark 2 is unique. The lower bound of N' is clearly $M_N - 1$. The problem of unicity will be deeply discussed in the Section II.

If (8) is fulfilled, the coefficient h_N can be retrieved by

$$h_N = \text{Ker}(\mathcal{L}_N) \quad (9)$$

Computing b_t

Let us recall the following definition:

Definition 1: [12] A *derivation* 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 $D(x.y) = xD(y)+yD(x)$.

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

$$Dp_N(z_k) = \frac{\partial p_N(z_k)}{\partial z_k} = \frac{\partial}{\partial z_k} \prod_{t=1}^N (z_k^T b_t) = \sum_{t=1}^N b_t \prod_{l \neq t} (z_k^T b_l) \quad (10)$$

We rewrite (10) as :

$$Dp_N(z_k) = b_t \prod_{l \neq t} (z_k^T b_l) + \sum_{i \neq t} b_i \prod_{j \neq i} (z_k^T b_j) \quad (11)$$

Now, consider an arbitrary vector $w_t \in \mathbb{F}_p^{K+2}$, such that, $w_t^T b_t = 0$. Replacing w_t ($t = 1, \dots, N$) into (11) yields:

$$Dp_N(w_t) = b_t \prod_{l \neq t} (w_t^T b_l) = b_t \cdot c \quad (12)$$

where c is a unknown scalar. Since $Dp_N(w_t)$ is known and the first component of b_t equals 1, the parameter vector b_t is obtained by merely normalizing $Dp_N(w_t)$ for $t = 1, \dots, N$. Hence, whenever the one-dimensionality of the solution h_N is guaranteed, its unicity, as well as the unicity of the b_t 's, are guaranteed. In the next Section, we discuss the unicity issue.

II. THE PE CONDITIONS REVISITED

We sum up the previous Section by stressing that the identification procedure requires to compute the solution of (7), that is finding out the kernel h_N of \mathcal{L}_N . The one-dimensionality of the solution is guaranteed by the rank condition (8). When working over \mathbb{R} , the assumption that the mapped regressor vectors $\nu_N(z_{k_i})$ are *sufficiently exciting* is known as the PE condition. On the other hand, over a finite field like \mathbb{F}_p , the PE conditions make no longer sense because the number of possible regressors z_{k_i} is finite. The objective of this subsection is to provide an alternative to the

PE conditions. They will be expressed in terms of necessary conditions.

Proposition 2: In order the kernel h_N to be one-dimensional, it is necessary that the triplet (p, K, N) fulfills

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

Proof: Let us first notice 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 $y_{k-1}, \dots, y_{k-K_1}, u_k, \dots, u_{k-K_2}$. These $K + 1$ components take value in the set \mathbb{F}_p which is of finite cardinality p .

Besides, 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 $\{\xi_k\}$ fulfills:

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

This implies :

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

Finally, considering both the relations (8) and (14) completes the proof. ■

The following Proposition allows to assess the impact of the triplet (p, K, N) on the unicity of the kernel.

Proposition 3: For all pairs (p, K_c) with $p \geq 2$, there exists an integer $N \in [1, N_{I/O}]$ so that :

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

for $K \geq K_c$

Proof: We 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

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

On the other hand, let us first show that for all $p \geq 2$ and for all K

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

It is clear that for all $p \geq 2$ we have:

$$\begin{aligned} p^{K+1} + 2 &> 2 \\ &\vdots \\ p^{K+1} + K + 1 &> K + 1 \end{aligned}$$

Multiplying all the terms in the left-hand side and the right-hand side yields:

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

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

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

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

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

and so

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

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

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

which proves (16).

Finally, it is easy to see that the functions $K \rightarrow p^{K+1}$ and $K \rightarrow M_N(K) - 1$ for any N are monotonic increasing functions of 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 $K \rightarrow p^{K+1}$ and $K \rightarrow M_N(K) - 1$ 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 Proposition 3 is useful to further investigate the impact of the pair (n, J) regarding the unicity of the solution. Indeed, K and N involved in the Proposition 3 are correlated respectively to the dimension n of the system (1) and its number J of modes. A graphical interpretation of the Proposition 3 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 lower than the curve $M_N(K) - 1$ prevent the condition (13) to be fulfilled and so the unicity of h_N .

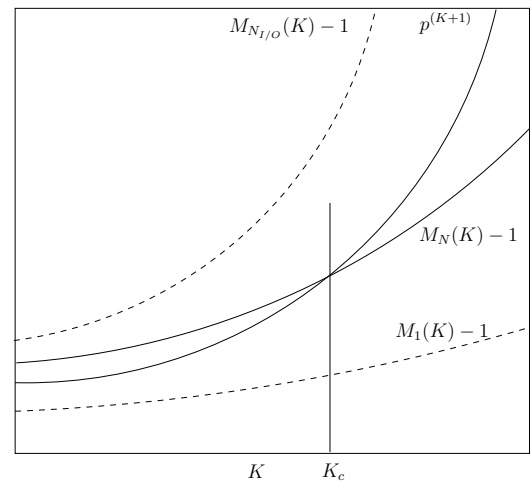


Fig. 1. Graphical interpretation of the Proposition 3

Remark 3: Even if (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} . Hence the maximal rank of the embedded data matrix may not reach $M_N(K) - 1$ preventing thereby the unicity of h_N .

III. PRACTICAL ISSUES AND EXAMPLES

A. Finding out the kernel

To find out the kernel in (9), we can resort to a Gaussian elimination over \mathbb{F}_p . Compared with the computation over \mathbb{R} , the method must be however 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 inverting over a finite field, the Extended Euclidean Algorithm [13] is particularly interesting. It is based on the computation of a *gcd* (greatest common divisor). The Extended Euclidean Algorithm for completing the multiplicative inverse of an integer denoted a is described below. It follows a Matlab syntax. Let $\mathcal{T}(i, j)$, $\mathcal{T}(i, :)$ denote respectively the component at i -th row and j -th column and the whole i -th row of the matrix \mathcal{T} defined as

$$\mathcal{T} = \begin{pmatrix} a & 1 & 0 \\ p & 0 & 1 \end{pmatrix}$$

Let $Quot(a, p)$ denote the quotient of the division $\frac{a}{p}$.

Algorithm 1 Extended Euclidean Algorithm

Input: a, p

Output: $inva \in \mathbb{F}_p$ % multiplicative inverse of a

Construct the matrix $\mathcal{T} = \begin{pmatrix} a & 1 & 0 \\ p & 0 & 1 \end{pmatrix}$

Set the variable $Continue = true$

while $Continue$ **do**

$tmpRow = \mathcal{T}(2, :)$

$\mathcal{T}(2, :) = \mathcal{T}(1, :) + \mathcal{T}(2, :) * (-Quot(\mathcal{T}(1, 1), \mathcal{T}(2, 1)))$

$\mathcal{T}(1, :) = tmpRow$

if $\mathcal{T}(2, 1) == 0$ **then** $Continue = false$

end if

end while

$inva = \mathcal{T}(1, 2)$ % multiplicative inverse of a

B. Finding out the points w_t

To determine the N distinct points w_t that lie on the N hyperplanes S_t , the following algebraic procedure can be carried out.

Consider a parameterized random line with direction v and a 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 intersections under the condition that it is not parallel with any of the hyperplanes. In other words, the equation of degree N

$$p_N(\mu v + w_0) = 0 \quad (17)$$

has N distinct integer roots $\{\mu_t\}_{t=1}^N$ under the constraint $p_N(v) \neq 0$ (or equivalently $v \notin S_t$). Therefore, the intersection of this line and all of the hyperplanes are given by:

$$w_t = \mu_t v + w_0 \quad \forall t \in \{1, \dots, N\}$$

Since w_t belongs to a finite field, an exhaustive search for finding out μ_t could be effective and would dispense from really solving the integer equation (17).

C. Examples

The purpose of this subsection is to illustrate through two simple examples the identification procedure over finite fields and the impact of the triplets $\{p, N, K\}$ regarding the unicity of the solution. The dimension $n = 1$ is considered but the results stated in this paper still holds for any dimension $n > 1$. The dimension n can be large if a cryptographic application is considered. Indeed, identification amounts to an attack in cryptography, that is a way of recovering the secret key played by the parameters of the dynamical system. It has been shown in [9] that the system (1) makes sense in cryptography since under flatness conditions, it acts as a so-called self-synchronizing stream cipher.

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 not accessible 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 input/output model reads:

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

The two parameter vectors are $b_1 = [1, -q_1, -5]^T$ and $b_2 = [1, -q_2, -5]^T$. Since $213 = -38 \pmod{251}$ and $246 = -5 \pmod{251}$ one has $b_1 = [1, 213, 246]^T$ 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 2, the maximum number of regressors is $N'_{max} = p^{K+1} = 251^{1+1} = 63001$. Besides, there exist two input/output relations according to the value of $q_{\sigma(k)}$. Hence, $N = 2$.

For $N = 2$ and $K = 1$, $M_N(K) - 1 = 5$. Thus, the necessary condition (13) is fulfilled. Consequently, it is possible that h_N is unique. So, we can proceed further.

Computing 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. A Gaussian elimination yields a unique kernel which reads after normalization (see Remark 2)

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

Computing b_t

First, we compute $N = 2$ points w_t so that $w_t^T b_t = 0$. Consider a random line with a direction $v = [25, 181, 61]^T$ and a base point $w_0 = [42, 155, 208]^T$.

Solving (17) yields $\mu_1 = 59$, $\mu_2 = 197$ and two corresponding intersections $w_1 = [11, 41, 42]^T$, $w_2 = [198, 170, 177]^T$.

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

$$\begin{aligned} b_1 &= [1, 213, 246]^T \\ b_2 &= [1, 38, 246]^T \end{aligned}$$

We obtain the right parameter vectors b_t . This results is explained by the fact that not only the necessary condition (13) is fulfilled but also because we have got enough independent regressor vectors.

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 input/output model reads:

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

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 2, the maximum number of regressors is $N'_{max} = p^{K+1} = 2^{1+1} = 4$. Besides, there exist two input/output relations according to the value of $q_{\sigma(k-1)}$. Hence, $N = 2$.

For $N = 2$ and $K = 1$, $M_N(K) - 1 = 5$. Thus, the necessary condition (13) is not fulfilled. Consequently, it is impossible that the kernel h_N is unique. It is explained by the fact that, regardless the dynamics, it is impossible to get enough independent regressor vectors.

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

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

To each kernel vector h_N , we can find the corresponding parameter vector b_t . Only the kernel vector $[1, 1, 0, 0, 1, 1]^T$ gives the right solution for the b_t '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. That explains why there are four distinct solutions in h_N : $M_N(K) - 2 = 6 - 2 = 4$.

IV. CONCLUDING REMARKS

From a theoretical point of view, the necessary condition proposed in this paper and guaranteeing the unicity does not take into account the dynamics of the system. Refining the bound by eliminating non admissible regressor vectors with respect to the dynamics would reduce the conservatism but finding out a priori the set of admissible vectors is not a trivial task and deserves deeper insights.

We have stressed that one of the motivation of the paper is using the identification procedure as an attack in a cryptographic application. The results provided in this paper have two major interests for such purpose. First, it is well-known that unicity in the parameters is a necessary condition for security. As a result, the conditions provided in this paper guarantee an admissible setting of the cipher in terms of dimension and number of modes. Furthermore, the security is related to the complexity of the identification procedure. The demanding task is the computation of the kernel of the embedded data matrix. It is obtained through a Gaussian elimination of which complexity is $O(\min(N' M_N^2, N'^2 M_N))$. The lower bound N' is $M_N - 1$ when M_N is large enough and the complexity can be approximated by $O(M_N^3)$.

REFERENCES

- [1] R. Shorten, F. Wirth, O. Mason, K. Wulff, and C. King. Stability criteria for switched and hybrid systems. *SIAM Rev.*, 49:545–592, 2005.
- [2] A. Benveniste and P. Le Guernic. Hybrid dynamical systems theory and nonlinear dynamical systems over finite fields. In *Proceedings. 27th IEEE Conference on Decision and Control CDC 1988*, Austin, TX, December 1988.
- [3] M. Le Borgne, A. Benveniste, and P. Le Guernic. Dynamical systems over galois fields and dedcs control problems. In *Proceedings. 30th IEEE Conference on Decision and Control CDC 1991*, Brighton, UK, December 1991.
- [4] 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.
- [5] E. Kasper, V. Rijmen, E. Bjorstad, C. Rechberger, M. Robshaw, and G. Sekar. Correlated keystreams in moustique. Technical report, ESTREAM Project, 2004.
- [6] P. Hawkes, M. Paddon, G. G. Rose, and W. V. Miriam. Primitive specification for sss. Technical report, e-Stream Project, 2004. Available at: <http://www.ecrypt.eu.org/stream/ciphers/sss/sss.pdf>.
- [7] G. Millérioux, J. M. Amigó, and J. Daafouz. A connection between chaotic and conventional cryptography. *IEEE Trans. on Circuits and Systems I: Regular Papers*, 55(6), July 2008.
- [8] G. Millérioux, P. Guillot, J. M. Amigó, and J. Daafouz. Flat dynamical systems and self-synchronizing stream ciphers. In *Proc. of the Fourth Workshop on Boolean Functions : Cryptography and Applications (BFCA'08)*, Copenhagen, Denmark, May 2008.
- [9] 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.
- [10] 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.
- [11] S. Paoletti, J. Roll, A. Garulli, and A. Vicino. Input/ouput realization of piecewise affine state space models. In *46th IEEE Conf. on Dec. and Control*, 2007.
- [12] S. Lang. *Algebra, Graduate Texts in Mathematics*. Berlin, New York: Springer-Verlag, 2002.
- [13] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.