Counting Equivalent Linear Finite Transducers Using a Canonical Form

Ivone Amorim, António Machiavelo, and Rogério Reis

CMUP, Faculdade de Ciências da Universidade do Porto
Rua do Campo Alegre, 4169-007 Porto, Portugal
{ivone.amorim,rvr}@dcc.fc.up.pt, ajmachia@fc.up.pt

Abstract. The notion of linear finite transducer (LFT) plays a crucial role in a family of cryptosystems introduced in the 80's and 90's. However, as far as we know, no study was ever conducted to count and enumerate these transducers, which is essential to verify if the size of the key space, of the aforementioned systems, is large enough to prevent an exhaustive search attack. In this paper, we determine the cardinal of the equivalence classes on the set of the LFTs with a given size. This result is sufficient to get an approximate value, by random sampling, for the number of non-equivalent injective LFTs, and subsequently for the size of the key space. We introduce a notion of canonical LFT, give a method to verify if two LFTs are equivalent, and prove that every LFT has exactly one equivalent canonical LFT. We then show how this canonical LFT allows us to calculate the size of each equivalence class on the set of the LFTs with the same number of states.

1 Introduction

Transducers, in the most used sense in automata theory, are automata with output that realise rational functions. They are widely studied in the literature, having numerous applications to real world problems. They are essential, for example, in language and speech processing [4].

In this work we deal only with transducers as defined by Renji Tao [7], and our motivation comes from their application to Cryptography. According to that definition, a transducer is a finite state sequential machine given by a quintuple $\langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$, where: $\mathcal{X}$, $\mathcal{Y}$ are the nonempty input and output alphabets, respectively; S is the nonempty finite set of states; $\delta : S \times \mathcal{X} \to S$, $\lambda : S \times \mathcal{X} \to \mathcal{Y}$, are the state transition and output functions, respectively. These transducers are deterministic and can be seen as having all the states as final. Every state in S can be used as initial, and this gives rise to a transducer in the usual sense, *i.e.*, one that realises a rational function. Therefore, in what follows, a transducer is a family of classical transducers that share the same underlying digraph.

A transducer is called linear if its transition and output functions are linear maps. These transducers play a core role in a family of cryptosystems, named FAPKCs, introduced in a series of papers by Tao [8,11,9,10]. Those schemes seem to be a good alternative to the classical ones, being computationally attractive

M. Holzer and M. Kutrib (Eds.): CIAA 2014, LNCS 8587, pp. 70–83, 2014.

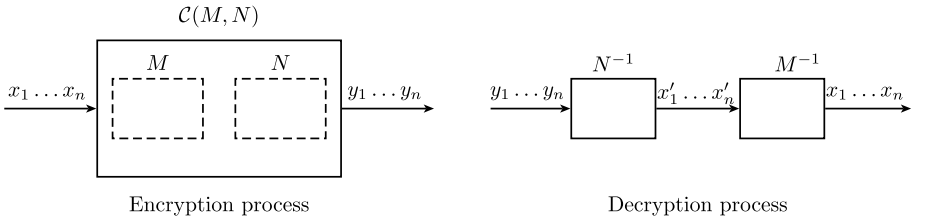

Fig. 1. Schematic representation of FAPKC working principle

and thus suitable for application on devices with very limited computational resources, such as satellites, cellular phones, sensor networks, and smart cards [9]. Roughly speaking, in these systems, the private key consists of two injective transducers, denoted by M and N in Figure 1, where M is a linear finite transducer (LFT), and N is a non-linear finite transducer (non-LFT) of a special kind, whose left inverses can be easily computed. The public key is the result of applying a special product for transducers, $\mathcal{C}$, to the original pair, thus obtaining a non-LFT, denoted by $\mathcal{C}(M,N)$ in Figure 1. The crucial point is that it is easy to obtain an inverse of $\mathcal{C}(M,N)$ from the inverses of its factors, M^{-1} and N^{-1}, while it is believed to be hard to find that inverse without knowing those factors. On the other hand, the factorization of a transducer seems to be hard by itself [12].

The LFTs in the FAPKC systems are of core importance in the invertibility theory of finite transducers, on which part of the security of these systems relies on [1]. They also play a crucial role in the key generation process, since in these systems a pair (public key, private key) is formed using a LFT and two non-LFTs, as explained above. Consequently, for these cryptosystems to be feasible, injective LFTs have to be easy to generate, and the set of non-equivalent injective LFTs has to be large enough to make an exhaustive search intractable.

Several studies were made on the invertibility of LFTs [5,6,13,12,3,1], and some attacks to the FAPKC systems were presented [2,13,7]. However, as far as we know, no study was conducted to determine the size of the key space of these systems. To evaluate that size, one first needs to determine the number of non-equivalent injective LFTs, the exact value of which seems to be quite hard to obtain. In order to be able to get an approximate value, one needs to know the different sizes of the equivalence classes. This is crucial to construct a LFT's uniform random generator.

In this work we describe a method to determine the sizes of those equivalence classes. To accomplish that, a notion of canonical LFT is introduced, being proved that each equivalence class has exactly one of these canonical LFTs. It is also shown how to construct the equivalent canonical LFT to any LFT in its matricial form, and, by introducing a new equivalence test for LFTs, to enumerate and count the equivalent transducers with the same number of states.

The paper is organized as follows. In Section 2 we introduce the basic definitions. Section 3 is devoted to the equivalence test on LFTs. The concept of

canonical LFTs is introduced in Section 4, and the results about the size of the LFTs equivalence classes are presented in Section 5.

2 Basic Concepts

As usual, for a finite set A, we let $|A|$ denote the cardinality of A, A^n be the set of words of A with length n, where $n \in \mathbb{N}$, and $A^0 = \{\varepsilon\}$, where ε denotes the empty word. We put $A^\star = \cup_{n\geq 0} A^n$, the set of all finite words, and $A^\omega = \{a_0 a_1 \cdots a_n \cdots \mid a_i \in A\}$ is the set of infinite words. Finally, $|\alpha|$ denotes the length of $\alpha \in A^\star$.

In what follows, a *finite transducer* (FT) is a finite state sequential machine which, in any given state, reads a symbol from a set $\mathcal{X}$, and produces a symbol from a set $\mathcal{Y}$, and switches to another state. Thus, given an initial state and a finite input sequence, a transducer produces an output sequence of the same length. The formal definition of a finite transducer is the following.

Definition 1. *A* finite transducer *is a quintuple $\langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda\rangle$, where: $\mathcal{X}$ is a nonempty finite set, called the* input alphabet*; $\mathcal{Y}$ is a nonempty finite set, called the* output alphabet*; S is a nonempty finite set called the* set of states*; $\delta : S \times \mathcal{X} \to S$, called the* state transition function*; and $\lambda : S \times \mathcal{X} \to \mathcal{Y}$, called the* output function*.*

Let $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda\rangle$ be a finite transducer. The state transition function δ and the output function λ can be extended to finite words, i.e., elements of $\mathcal{X}^\star$, recursively, as follows:

$$\begin{aligned} \delta(s,\varepsilon) &= s & \qquad \delta(s,x\alpha) &= \delta(\delta(s,x),\alpha) \\ \lambda(s,\varepsilon) &= \varepsilon & \qquad \lambda(s,x\alpha) &= \lambda(s,x)\,\lambda(\delta(s,x),\alpha), \end{aligned}$$

where $s \in S$, $x \in \mathcal{X}$, and $\alpha \in \mathcal{X}^\star$. In an analogous way, λ may be extended to $\mathcal{X}^\omega$.

From these definitions it follows that, for all $s \in S, \alpha \in \mathcal{X}^\star$, and for all $\beta \in \mathcal{X}^\star \cup \mathcal{X}^\omega$,

$$\lambda(s,\alpha\beta) = \lambda(s,\alpha)\,\lambda(\delta(s,\alpha),\beta).$$

The notions of equivalent states and minimal transducer considered here are the classical ones.

Definition 2. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}_1, S_1, \delta_1, \lambda_1\rangle$ and $M_2 = \langle \mathcal{X}, \mathcal{Y}_2, S_2, \delta_2, \lambda_2\rangle$ be two FTs. Let $s_1 \in S_1$, and $s_2 \in S_2$. One says that s_1 and s_2 are* equivalent*, and denote this relation by $s_1 \sim s_2$, if*

$$\forall \alpha \in \mathcal{X}^\star,\ \lambda_1(s_1,\alpha) = \lambda_2(s_2,\alpha).$$

Definition 3. *A finite tranducer is called* minimal *if it has no pair of equivalent states.*

We now introduce the notion of equivalent transducers used in this context.

Definition 4. *M_1 and M_2 are said to be* equivalent*, denoted by $M_1 \sim M_2$, if the following two conditions are satisfied:*

$$\forall s_1 \in S_1,\ \exists s_2 \in S_2 :\ s_1 \sim s_2 \ \text{ and } \ \forall s_2 \in S_2,\ \exists s_1 \in S_1 :\ s_1 \sim s_2.$$

This relation $\sim$ defines an equivalence relation on the set of FTs.

Definition 5. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}, S_1, \delta_1, \lambda_1 \rangle$ and $M_2 = \langle \mathcal{X}, \mathcal{Y}, S_2, \delta_2, \lambda_2 \rangle$ be two FTs. M_1 and M_2 are said to be* isomorphic *if there exists a bijective map ψ from S_1 onto S_2 such that*

$$\begin{aligned} \psi(\delta_1(s_1, x)) &= \delta_2(\psi(s_1), x) \\ \lambda_1(s_1, x) &= \lambda_2(\psi(s_1), x) \end{aligned}$$

for all $s_1 \in S_1$, and for all $x \in X$. The map ψ is called an isomorphism *from M_1 to M_2.*

Finally, we give the definition of linear finite transducer (LFT).

Definition 6. *If $\mathcal{X}, \mathcal{Y}$ and S are vector spaces over a field $\mathbb{F}$, and both $\delta : S \times \mathcal{X} \to S$ and $\lambda : S \times \mathcal{X} \to Y$ are linear maps, then $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$ is called* linear *over $\mathbb{F}$, and we say that $dim(S)$ is the size of M.*

Let $\mathcal{L}$ be the set of LFTs over $\mathbb{F}$, and $\mathcal{L}_n$ the set of the transducers in $\mathcal{L}$ with size n. The restriction of $\sim$ to $\mathcal{L}$ is also represented by $\sim$, and the restriction to $\mathcal{L}_n$ is denoted by $\sim_n$.

Definition 7. *Let M_1 and M_2 be two LFTs. M_1 and M_2 are said to be* similar *if there is a linear isomorphism from M_1 to M_2.*

Let $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$ be a LFT over a field $\mathbb{F}$. If $\mathcal{X}, \mathcal{Y}$, and S have dimensions l, m and n, respectively, then there exist matrices $A \in \mathcal{M}_{n,n}(\mathbb{F})$, $B \in \mathcal{M}_{n,l}(\mathbb{F})$, $C \in \mathcal{M}_{m,n}(\mathbb{F})$, and $D \in \mathcal{M}_{m,l}(\mathbb{F})$, such that

$$\begin{aligned} \delta(s, x) &= As + Bx, \\ \lambda(s, x) &= Cs + Dx, \end{aligned}$$

for all $s \in S$, $x \in \mathcal{X}$. The matrices A, B, C, D are called the *structural matrices* of M, and l, m, n are called its *structural parameters*. Notice that if M_1 and M_2 are two equivalent LFTs with structural parameters l_1, m_1, n_1 and l_2, m_2, n_2, respectively, then, from the definition of equivalent transducers, one has $l_1 = l_2$ and $m_1 = m_2$.

A LFT such that C is the null matrix (with the adequate dimensions) is called *trivial*.

One can associate to a LFT, M, with structural matrices A, B, C, D, a family of matrices which are very important in the study of its equivalence class, as will be clear throughout this paper.

Definition 8. *Let $M \in \mathcal{L}_n$ with structural matrices A, B, C, D. The matrix*

$$\Delta_M^{(k)} = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{k-1} \end{bmatrix}$$

is called the k-diagnostic matrix *of M, where $k \in \mathbb{N} \cup \{\infty\}$.*

The matrix $\Delta_M^{(n)}$ will be simply denoted by Δ_M and will be referred to as the *diagnostic matrix* of M. The matrix $\Delta_M^{(2n)}$ will be denoted by $\hat{\Delta}_M$ and called the *augmented diagnostic matrix* of M.

Definition 9. *Let V be a k-dimensional vector subspace of $\mathbb{F}^n$, where $\mathbb{F}$ is a field. The unique basis $\{b_1, b_2, \ldots, b_k\}$ of V such that the matrix $[b_1\ b_2\ \cdots\ b_k]^T$ is in row echelon form will be here referred to as the* standard basis *of V.*

3 Testing the Equivalence of LFTs

Let $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$ be a LFT over a field $\mathbb{F}$ with structural matrices A, B, C, D. Starting at a state s_0 and reading an input sequence $x_0x_1x_2\ldots$, one gets a sequence of states $s_0s_1s_2\ldots$ and a sequence of outputs $y_0y_1y_2\ldots$ satisfying the relations

$$\begin{aligned} s_{t+1} &= \delta(s_t, x_t) = As_t + Bx_t, \\ y_t &= \lambda(s_t, x_t) = Cs_t + Dx_t, \end{aligned}$$

for all $t \geq 0$. The following result is then easily proven by induction [7, Theorem 1.3.1].

Theorem 1. *For a LFT as above, $s_{i+1} = A^i s_0 + \sum_{j=0}^{i-1} A^{i-j-1}Bx_j$, and $y_i = CA^i s_0 + \sum_{j=0}^{i} H_{i-j}x_j$, for $i \in \{0, 1, \ldots\}$, where $H_0 = D$, and $H_j = CA^{j-1}B$, $j > 0$.*

Tao, in his book, presents the following necessary and sufficient condition, the only one known so far, for the equivalence of two states of LFTs [7, Theorem 1.3.3]:

Theorem 2. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}_1, S_1, \delta_1, \lambda_1 \rangle$ and $M_2 = \langle \mathcal{X}, \mathcal{Y}_2, S_2, \delta_2, \lambda_2 \rangle$ be two LFTs. Let $s_1 \in S_1$, and $s_2 \in S_2$. Then, $s_1 \sim s_2$ if and only if the null states of M_1 and M_2 are equivalent, and $\lambda_1(s_1, 0^\omega) = \lambda_2(s_2, 0^\omega)$.*

And, as a consequence, he also presents a necessary and sufficient condition for the equivalence of two LFTs [7, Theorem 1.3.3]:

Corollary 1. *Let M_1 and M_2 be two LFTs. Then, $M_1 \sim M_2$ if and only if their null states are equivalent, and $\{\lambda_1(s_1, 0^\omega) \mid s_1 \in S_1\} = \{\lambda_2(s_2, 0^\omega) \mid s_2 \in S_2\}$.*

However, both conditions cannot be checked efficiently, since they involve working with infinite words. In this section, we explain how they can be reduced to a couple of conditions that can effectively be verified. These new results will be essential in Section 5 to compute the sizes of the equivalence classes in $\mathcal{L}_n/\sim_n$.

The following two Lemmas, which play an important role in the proofs of the subsequent results, are immediate consequences of the basic fact that right multiplication performs linear combinations on the columns of a matrix.

Lemma 1. *Let $A \in \mathcal{M}_{m\times k}$, and $B \in \mathcal{M}_{m\times l}$. Then,* $\mathrm{rank}([A|B]) = \mathrm{rank}(A)$ *if and only if there $X \in \mathcal{M}_{k\times l}$ such that $B = AX$.*

Lemma 2. *Let $A, B \in \mathcal{M}_{m\times k}$. Then,* $\mathrm{rank}(A) = \mathrm{rank}([A|B]) = \mathrm{rank}(B)$ *if and only if there is an invertible matrix $X \in \mathcal{M}_{k\times k}$ such that $B = AX$.*

For the remainder of this Section, let M_1, M_2 be two LFTs with structural matrices A_1, B_1, C_1, D_1, and A_2, B_2, C_2, D_2 respectively. Let l_1, m_1, n_1 be the structural parameters of M_1, and l_2, m_2, n_2 be the structural parameters of M_2. To simplify the notation, take $\tilde{\Delta}_1 = \Delta_{M_1}^{(n_1+n_2)}$ and $\tilde{\Delta}_2 = \Delta_{M_2}^{(n_1+n_2)}$.

Lemma 3. *Let $s_1 \in S_1$ and $s_2 \in S_2$. Then, $\lambda_1(s_1, 0^\omega) = \lambda_2(s_2, 0^\omega)$ if and only if $\tilde{\Delta}_1 s_1 = \tilde{\Delta}_2 s_2$.*

Proof. From Theorem 1, one has that $\lambda_1(s_1, 0^\omega) = \lambda_2(s_2, 0^\omega)$ if and only if $C_1 A_1^i s_1 = C_2 A_2^i s_2$, for $i \geq 0$. Let p_1 be the characteristic polynomial of A_1, and p_2 the characteristic polynomial of A_2. Then, p_1 and p_2 are monic polynomials of order n_1 and n_2, respectively. Moreover, by the Cayley-Hamilton theorem, $p_1(A_1) = p_2(A_2) = 0$. Thus, $p = p_1 p_2$ is a monic polynomial of order $n_1 + n_2$ such that $p(A_1) = p(A_2) = 0$. Therefore $A_1^{n_1+n_2+k}$ and $A_2^{n_1+n_2+k}$, with $k \geq 0$, are linear combinations of lower powers of A_1 and A_2, respectively, with the same coefficients. Consequently, $C_1 A_1^i s_1 = C_2 A_2^i s_2$ for $i \geq 0$ is equivalent to $C_1 A_1^i s_1 = C_2 A_2^i s_2$ for $i = 0, 1, \ldots, n_1 + n_2 - 1$, and the result follows. □

The next result states that the (n_1+n_2)-diagnostic matrices of two equivalent LFTs, of sizes n_1 and n_2, can be used to verify if two of their states are equivalent. It follows from the previous Lemma, and from the fact that if $M_1 \sim M_2$ then, by Theorem 2, $s_1 \sim s_2$ if and only if $\lambda_1(s_1, 0^\omega) = \lambda_2(s_2, 0^\omega)$.

Theorem 3. *Let $s_1 \in S_1$ and $s_2 \in S_2$. If $M_1 \sim M_2$, then $s_1 \sim s_2$ if and only if $\tilde{\Delta}_1 s_1 = \tilde{\Delta}_2 s_2$.*

Corollary 2. *Let M be a LFT, and $s_1, s_2 \in M$. Then, $s_1 \sim s_2$ if and only if $\Delta_M s_1 = \Delta_M s_2$.*

Proof. From the last Theorem, $s_1 \sim s_2$ if and only if $\hat{\Delta}_M s_1 = \hat{\Delta}_M s_2$, that is, if and only if $CA^i s_1 = CA^i s_2$, for $i = 0, 1, \ldots, 2n-1$. Since the minimal polynomial of A has, at most, degree n, this latter condition is equivalent to $CA^i s_1 = CA^i s_2$, for $i = 0, 1, \ldots, n-1$. Thus, $s_1 \sim s_2$ if and only if $\Delta_M s_1 = \Delta_M s_2$. □

Corollary 3. *Let M be a LFT over a field $\mathbb{F}$. Then M is minimal if and only if* $\operatorname{rank}(\Delta_M) = \operatorname{size}(M)$.

Proof. It is enough to notice that the linear application $\varphi : S/\!\sim \to \mathbb{F}^{nm}$ defined by $\varphi([\, s \,]_\sim) = \Delta_M s$ is well-defined and injective, by the previous Corollary. □

The following theorem gives a pair of conditions that have to be satisfied for two LFTs to be equivalent.

Theorem 4. *For LFTs M_1 and M_2 as above, $M_1 \sim M_2$ if and only if the following two conditions are simultaneously verified:*

1. $\operatorname{rank}(\tilde{\Delta}_1) = \operatorname{rank}([\tilde{\Delta}_1 \mid \tilde{\Delta}_2]) = \operatorname{rank}(\tilde{\Delta}_2)$;
2. $D_1 = D_2$ *and* $\tilde{\Delta}_1 B_1 = \tilde{\Delta}_2 B_2$.

Proof. From Corollary 1 one has that $M_1 \sim M_2$ if and only if the null states of M_1 and M_2 are equivalent, and $\{\lambda_1(s_1, 0^\omega) \mid s_1 \in S_1\} = \{\lambda_2(s_2, 0^\omega) \mid s_2 \in S_2\}$.

The null states of M_1 and M_2 are equivalent if and only if $\forall \alpha \in \mathcal{X}^\star$, $\lambda_1(0, \alpha) = \lambda_2(0, \alpha)$. By Theorem 1, this is equivalent to: $\sum_{j=0}^{i} H_{i-j} x_j = \sum_{j=0}^{i} H'_{i-j} x_j$, $i = 0, 1, \ldots, |\alpha|$, where $\alpha = x_0 x_1 \cdots x_{|\alpha|} \in \mathcal{X}^\star$, $H_0 = D_1$, $H'_0 = D_2$ and $H_j = C_1 A_1^{j-1} B_1$, $H'_j = C_2 A_2^{j-1} B_2$, for $j > 0$. That is, $\forall x_0, x_1, \cdots, x_{|\alpha|} \in \mathcal{X}$ the following equations are simultaneously satisfied:

$$
\begin{aligned}
D_1 x_0 &= D_2 x_0 \\
D_1 x_1 + C_1 B_1 x_0 &= D_2 x_1 + C_2 B_2 x_0 \\
D_1 x_2 + C_1 B_1 x_1 + C_1 A_1 B_1 x_0 &= D_2 x_2 + C_2 B_2 x_1 + C_2 A_2 B_2 x_0 \\
&\vdots \\
D_1 x_{|\alpha|} + \cdots + C_1 A_1^{(|\alpha|-1)} B_1 x_0 &= D_2 x_{|\alpha|} + \cdots + C_2 A_2^{(|\alpha|-1)} B_2 x_0.
\end{aligned}
$$

Using the characteristic polynomials of A_1 and A_2, as in the proof of Lemma 3, one sees that when $|\alpha| \geq u$ the equations after the first u of them are implied by the previous ones. From the arbitrariness of α, it then follows that system is satisfied if and only if $D_1 = D_2$ and $\tilde{\Delta}_1 B_1 = \tilde{\Delta}_2 B_2$.

From Lemma 3, one has that $\{\lambda_1(s_1, 0^\omega) \mid s_1 \in S_1\} = \{\lambda_2(s_2, 0^\omega) \mid s_2 \in S_2\}$ if and only if $\{\tilde{\Delta}_1 s_1 \mid s_1 \in S_1\} = \{\tilde{\Delta}_2 s_2 \mid s_2 \in S_2\}$. This means that the column space of $\tilde{\Delta}_1$ is equal to the column space of $\tilde{\Delta}_2$, which is true if and only if there exist matrices X, Y such that $\tilde{\Delta}_2 = \tilde{\Delta}_1 X$ and $\tilde{\Delta}_1 = \tilde{\Delta}_2 Y$. But, from Lemma 1, this happens if and only if $\operatorname{rank}(\tilde{\Delta}_1) = \operatorname{rank}([\tilde{\Delta}_1 \mid \tilde{\Delta}_2])$ and $\operatorname{rank}(\tilde{\Delta}_2) = \operatorname{rank}([\tilde{\Delta}_1 \mid \tilde{\Delta}_2])$. □

Using the conditions in the previous result, it is not hard to write an algorithm to test the equivalence of two LFTs. The running time of such an algorithm will be of the same order as the running time of well known algorithms to compute the rank of a matrix.

Corollary 4. $M_1 \sim M_2$ *implies* $D_1 = D_2$.

It is important to recall, at this moment, that the size of an LFT is the only structural parameter that can vary between transducers of the same equivalence class in $\mathcal{L}/\sim$. Moreover, the size of an LFT of an equivalence class $[M]_\sim$, can never be smaller than $\text{rank}(\Delta_{M'})$, where M' is a minimal transducer in $[M]_\sim$. These facts will be important in Section 5.

The following Corollary is a direct consequence of Lemma 2 and of the first point of Theorem 4.

Corollary 5. *If $n = n_1 = n_2$, $S_1 = S_2$, and $M_1 \sim M_2$, then there is an invertible matrix $X \in \mathcal{M}_{n\times n}$ such that $\hat{\Delta}_{M_2} = \hat{\Delta}_{M_1} X$.*

4 Canonical LFTs

In this section we prove that every equivalence class in $\mathcal{L}/\sim$ has one and only one LFT that satisfies a certain condition[1]. We also prove that, given the structural matrices of a LFT, M, one can identify and construct the transducer in $[M]_\sim$ that satisfies that aforesaid condition. LFTs that satisfy that condition are what we call *canonical* LFTs.

Lemma 4. *Let $M \in \mathcal{L}_n$ with structural matrices A, B, C, D. Then,*

$$\text{rank}(\Delta_M^{(k)}) = \text{rank}(\Delta_M),\ \forall k \geq n.$$

Proof. The degree of the minimal polynomial of A is at most n, and so the matrices CA^k, for $k \geq n$, are linear combinations of $C, CA^1, \cdots, CA^{n-1}$. □

The following result shows that if two minimal LFTs, with the same set of states, are equivalent, then the two vector spaces generated by the columns of their diagnostic matrices are equal.

Corollary 6. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_1, \lambda_1\rangle$ and $M_2 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_2, \lambda_2\rangle$ be two minimal LFT such that $M_1 \sim M_2$. Then, $\{\Delta_{M_1} s \mid s \in S\} = \{\Delta_{M_2} s \mid s \in S\}$.*

Proof. If $M_1 \sim M_2$, then $\{\lambda_1(s, 0^\omega) \mid s \in S\} = \{\lambda_2(s, 0^\omega) \mid s \in S\}$, by Corollary 1. That is, $\{\Delta_{M_1}^{(\infty)} s \mid s \in S\} = \{\Delta_{M_2}^{(\infty)} s \mid s \in S\}$. Since M_1 and M_2 are minimal, from Lemma 4 and Corollary 3 one concludes that $\{\Delta_{M_1} s \mid s \in S\} = \{\Delta_{M_2} s \mid s \in S\}$. □

If M is a minimal LFT, then the columns of Δ_M form a basis of the space $\{\Delta_M s \mid s \in S\}$. Therefore, if M_1 and M_2 are minimal and equivalent, there is an invertible matrix X (with adequate dimensions) such that $\Delta_{M_1} X = \Delta_{M_2}$. Note that this condition, here obtained for minimal transducers, is less demanding than the one we have in Corollary 5.

The next result, together with its proof, gives a way to generate LFTs in $[M]_\sim$, where M is a LFT defined by its structural matrices.

[1] The equivalence classes formed by trivial LFTs are excluded.

Lemma 5. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_1, \lambda_1 \rangle$ be a non-trivial LFT. Let $\psi : S \to S$ be a vector space isomorphism. Then, there is exactly one LFT $M_2 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_2, \lambda_2 \rangle$ such that ψ is a linear isomorphism from M_1 to M_2. Moreover, M_1 is minimal if and only if M_2 is minimal.*

Proof. Let P be the matrix of ψ relative to the standard basis. From its definition ψ is an isomorphism between M_1 and M_2 if and only the conditions mentioned in Section 2 are satisfied. Let $x = 0$ and $s_1 \in S$. From the first condition, one gets

$$\psi(\delta_1(s_1, 0)) = \delta_2(\psi(s_1), 0) \Leftrightarrow PA_1 s_1 = A_2 P s_1 \Leftrightarrow (PA_1 - A_2 P)s_1 = 0.$$

From the arbitrariness of s_1, this is equivalent to $PA_1 - A_2 P = 0$. Since P is invertible, one gets $A_2 = PA_1 P^{-1}$. The second condition yields

$$\lambda_1(s_1, 0) = \lambda_2(\psi(s_1), 0) \Leftrightarrow C_1 s_1 = C_2 P s_1 \Leftrightarrow (C_1 - C_2 P)s_1 = 0.$$

Again, from the arbitrariness of s_1, this is equivalent to $C_1 - C_2 P = 0$. Thus, $C_2 = C_1 P^{-1}$.

Now, let $s_1 = 0$ and $x \in X$. Using a similar method, one gets $B_2 = PB_1$ and $D_1 = D_2$. Hence, the transducer M_2 satisfying the conditions of the theorem is uniquely determined by ψ. It is then easy to see that the transducer given by the structural matrices $A_2 = PA_1 P^{-1}$, $B_2 = PB_1$, $C_2 = C_1 P^{-1}$, and $D_2 = D_1$ is such that ψ is a linear isomorphism from M_1 to M_2.

Since M_1 and M_2 are isomorphic, they are equivalent. Therefore, M_1 is minimal if and only if M_2 is minimal. □

Recalling that $GL_n(\mathbb{F})$ denotes the set of $n \times n$ invertible matrices over the field $\mathbb{F}$, one has:

Corollary 7. *Let $M \in \mathcal{L}_n$ be a non-trivial minimal LFT over a finite field $\mathbb{F}$. Then, the number of minimal LFTs in $[M]_\sim$ is $|GL_n(\mathbb{F})|$.*

Moreover, from the proof of Lemma 5, one gets that, given an invertible matrix X, there is exactly one minimal transducer in $[M]_\sim$ which has $\Delta_M X$ as diagnostic matrix. The same is not true if M is not minimal, as it will be shown in the next section. The aforementioned proof also gives an explicit way to obtain that transducer from the structural matrices of M.

Proposition 1. *Let $M_1 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_1, \lambda_1 \rangle$ be a LFT. Let $\psi : S \to S$ be a vector space isomorphism. Let M_2 be the LFT constructed from M_1 and $\psi(s) = Ps$ as described in the proof of the last Theorem. Then, $\Delta_{M_1} s = \Delta_{M_2} \psi(s)$.*

Proof. Let $s \in S$, then

$$\Delta_{M_2} \psi(s) = \begin{bmatrix} C_1 P^{-1} \\ C_1 A_1 P^{-1} \\ \vdots \\ C_1 A_1^{n-1} P^{-1} \end{bmatrix} Ps = \begin{bmatrix} C_1 \\ C_1 A_1 \\ \vdots \\ C_1 A_1^{n-1} \end{bmatrix} s = \Delta_{M_1} s.$$

□

The next Theorem gives the condition that was promised at the beginning of this section.

Theorem 5. *Every non-trivial equivalence class in $\mathcal{L}/\sim$ has exactly one LFT $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$ which satisfies the condition that $\{\Delta_M e_1, \Delta_M e_2, \cdots, \Delta_M e_n\}$ is the standard basis of $\{\Delta_M s \mid s \in S\}$, where $\{e_1, e_2, \cdots, e_n\}$ is the standard basis of S.*

Proof. Given the structural matrices of a LFT, Tao shows [7, Theorem 1.3.4] how to compute an equivalent minimal LFT. This implies, in particular, that every LFT is equivalent to a minimal LFT. Thus, to get the result here claimed, it is enough to prove that if $M_1 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_1, \lambda_1 \rangle$ is a non-trivial minimal LFT, then M_1 is equivalent to exactly one finite transducer $M_2 = \langle \mathcal{X}, \mathcal{Y}, S, \delta_2, \lambda_2 \rangle$ such that $\{\Delta_{M_2} e_1, \Delta_{M_2} e_2, \ldots, \Delta_{M_2} e_n\}$ is the standard basis of $\{\Delta_{M_1} s \mid s \in S\}$. First, let us notice that, since M_1 is minimal, Δ_{M_1} is left invertible, and consequently s is uniquely determined by $\Delta_{M_1} s$. Let $\mathcal{B} = \{b_1, b_2, \cdots, b_n\}$ be the standard basis of $\{\Delta_{M_1} s \mid s \in S\}$. Let s_i be the unique vector in S such that $b_i = \Delta_{M_1} s_i$, for $i = 1, 2, \ldots, n$. Let $\psi : S \to S$ be defined by $\psi(s_i) = e_i$. Then ψ is a vector space isomorphism. Let M_2 be the LFT constructed from M_1 and ψ as described in the proof of Lemma 5. Then, $M_2 \sim M_1$ and M_2 is minimal, which, by Corollary 6, implies $\{\Delta_{M_2} s \mid s \in S\} = \{\Delta_{M_1} s \mid s \in S\}$. From Proposition 1 one also has $\Delta_{M_2} e_i = \Delta_{M_2} \psi(s_i) = \Delta_{M_1} s_i = b_i$, for $i = 1, 2, \cdots, n$. Therefore, $\{\Delta_{M_2} e_1, \Delta_{M_2} e_2, \ldots, \Delta_{M_2} e_n\}$ is the standard basis of $\{\Delta_{M_1} s \mid s \in S\}$. The uniqueness easily follows from the fact that all choices made are unique. □

Finally we can state the definition of canonical LFT here considered.

Definition 10. *Let $M = \langle \mathcal{X}, \mathcal{Y}, S, \delta, \lambda \rangle$ be a linear finite transducer. One says that M is a* canonical LFT *if $\{\Delta_M e_1, \Delta_M e_2, \cdots, \Delta_M e_n\}$ is the standard basis of $\{\Delta_M s \mid s \in S\}$, where $\{e_1, e_2, \cdots, e_n\}$ is the standard basis of S.*

The proofs of Theorem 5 and Lemma 5 show that given the structural matrices of a LFT, M, one can identify and construct the canonical transducer in $[M]_\sim$.

5 On the Size of Equivalence Classes of LFTs

In what follows we only consider LFTs defined over finite fields with q elements, $\mathbb{F}_q$, because these are the ones commonly used in Cryptography.

In this section we explore how the size of the equivalence classes in $\mathcal{L}_n/\sim_n$ varies with the size n. Given a minimal LFT M_1 in $\mathcal{L}_{n_1}$, our aim is to count the number of transducers in $\mathcal{L}_{n_2}$, with $n_2 \geq n_1$, that are equivalent to M_1.

The following result shows that given $M_1 \in \mathcal{L}_{n_1}$, one can easily construct an equivalent transducer in $\mathcal{L}_{n_2}$, for any $n_2 \geq n_1$, which can then be used to count the number of transducers in $\mathcal{L}_{n_2}$ that are equivalent to M_1, as well as the size of the equivalence classes in S.

Proposition 2. *Let M_1 be the LFT over $\mathbb{F}_q$ with structural matrices A_1, B_1, C_1, D_1, and structural parameters l, m, n_1. Let $n' \in \mathbb{N}$, and M_2 be the LFT with structural matrices*

$$A_2 = \left[\begin{array}{c:c} A_1 & 0_{n_1 \times n'} \\ \hdashline 0_{n' \times n_1} & 0_{n' \times n'} \end{array}\right],\ B_2 = \begin{bmatrix} B_1 \\ 0_{n' \times l} \end{bmatrix},\ C_2 = \begin{bmatrix} C_1 & 0_{m \times n'} \end{bmatrix},\ \text{and } D_2 = D_1.$$

Then, $M_1 \sim M_2$. The structural parameters of M_2 are l, m, n_2, where $n_2 = n_1 + n'$.

Proof. Take $u = n_1 + n_2$. Notice that $C_2 A_2^i = [C_1 A_1^i \quad 0_{m \times n'}]$, for $i = 0, 1, \ldots, u-1$. That is, $\Delta_{M_2}^{(u)} = [\Delta_{M_1}^{(u)} \quad 0_{um \times n'}]$. The result is then trivial by Theorem 4. □

The next result counts the number of LFTs in $\mathcal{L}_{n_2}$ that are equivalent to M_2, where M_2 is the LFT defined from M_1 as described in Proposition 2. Because $M_1 \sim M_2$, this yields the number of LFTs in $\mathcal{L}_{n_2}$ that are equivalent to M_1.

Theorem 6. *Let M_1 be a minimal LFT in $\mathcal{L}_{n_1}$ with structural matrices A_1, B_1, C_1, D_1, and structural parameters l, m, n_1. Let M_2 be the LFT described in Proposition 2. The number of finite transducers $M \in \mathcal{L}_{n_2}$ which are equivalent to M_2 is $(q^{n_2} - 1)(q^{n_2} - q) \cdots (q^{n_2} - q^{r-1}) q^{(n_2+l)(n_2-r)}$, where $r = \operatorname{rank}(\hat{\Delta}_{M_2})$.*

Proof. The theorem follows from the next three facts, that we will prove in the remaining of this section.

1. For all matrices $\Delta_1, \Delta_2 \in \{\hat{\Delta}_M \mid M \in \mathcal{L}_{n_2} \text{ and } M \sim M_2\}$, the number of LFTs that are equivalent to M_2 and have Δ_1 as augmented diagnostic matrix is equal to the number of LFTs that are equivalent to M_2 and have Δ_2 as augmented diagnostic matrix.
2. The number of LFTs equivalent to M_2 and have $\hat{\Delta}_{M_2}$ as augmented diagnostic matrix is $q^{(n_2+l)(n_2-r)}$, with $r = \operatorname{rank}(\hat{\Delta}_{M_2})$.
3. The size of $\{\hat{\Delta}_M \mid M \in \mathcal{L}_{n_2} \text{ and } M \sim M_2\}$ is $(q^{n_2}-1)(q^{n_2}-2)\cdots(q^{n_2}-q^{r-1})$, with $r = \operatorname{rank}(\hat{\Delta}_{M_2})$.

□

From Corollary 5, if two LFTs M and M' are equivalent, there is an invertible matrix X such that $\Delta_{M'} = \Delta_M X$. The first of the above items is then an instance of the following result.

Theorem 7. *Let $M \in \mathcal{L}_n$. Let $S_\Delta = \{M' \in \mathcal{L}_n \mid M' \sim M \text{ and } \hat{\Delta}_{M'} = \Delta\}$. Then, for every $X \in GL_n(\mathbb{F}_q)$, $|S_{\hat{\Delta}_M}| = |S_{\hat{\Delta}_M X}|$.*

Proof. Let $f : S_{\Delta_M} \to S_{\Delta_M X}$ such that $f(M) = M'$, where M' is the transducer defined by the matrices $A' = X^{-1}AX$, $B' = X^{-1}B$, $C' = CX$ and $D' = D$. It is straightforward to see that $\hat{\Delta}_{M'} = \hat{\Delta}_M X$, and that the application f is bijective. □

To prove item 2, let us count the number of transducers $M \in \mathcal{L}_{n_2}$ that are equivalent to M_2 and have $\hat{\Delta}_{M_2}$ as augmented diagnostic matrix. One has to count the possible choices for the structural matrices A, B, C and D, of M, that satisfy the condition 2 of Theorem 4, and $\hat{\Delta}_{M_2} = \hat{\Delta}_M$ (which implies condition 1). The choice for D is obvious and unique from condition 2, as well as the choice for C (from condition $\hat{\Delta}_{M_2} = \hat{\Delta}_M$). How many choices does one have for A such that the condition $\hat{\Delta}_{M_2} = \hat{\Delta}_M$ is satisfied? And, how many choices for B such that $\hat{\Delta}_{M_2} = \hat{\Delta}_M$ and the second condition is satisfied, *i.e.*, such that $\hat{\Delta}_M B_2 = \hat{\Delta}_M B$? The following result gives the number of possible choices for A, and the proof gives the form of these matrices.

Theorem 8. *Let M_1 be a minimal LFT in $\mathcal{L}_{n_1}$ with structural matrices A_1, B_1, C_1, D_1, and M_2 the LFT described in Proposition 2. There are exactly $q^{n_2\left(n_2-\operatorname{rank}(\Delta_{M_2})\right)}$ matrices $A \in \mathcal{M}_{n_2\times n_2}(\mathbb{F}_q)$ such that $C_2A_2^i = C_2A^i$, for $i = 0, 1, \cdots, 2n_2 - 1$.*

Proof. Let $A \in \mathcal{M}_{n_2\times n_2}(\mathbb{F}_q)$ be such that $C_2A_2^i = C_2A^i$, for $i = 0, 1, \ldots, 2n_2-1$. Then, $C_2A_2^i = C_2A_2^{i-1}A$, for $i = 0, 1, \ldots, 2n_2 - 1$.

Take $A = \left[\begin{array}{c|c} E_1 & E_2 \\ \hline E_3 & E_4 \end{array}\right]$, with $E_1 \in \mathcal{M}_{n_1\times n_1}(\mathbb{F}_q)$, $E_2 \in \mathcal{M}_{n_1\times n'}(\mathbb{F}_q)$, $E_3 \in \mathcal{M}_{n'\times n_1}(\mathbb{F}_q)$, $E_4 \in \mathcal{M}_{n'\times n'}(\mathbb{F}_q)$, and $n' = n_2-n_1$. Then, from $C_2A_2^i = C_2A_2^{i-1}A$, for $i \in \{1, \ldots, 2n_2 - 1\}$, one gets that $\left[C_1A_1^i\ 0_{m\times n'}\right] = \left[C_1A_1^{i-1}E_1\ C_1A_1^{i-1}E_2\right]$, for $i \in \{1, \ldots, 2n_2 - 1\}$, *i.e.*, $C_1A_1^i = C_1A_1^{i-1}E_1$, and $C_1A_1^{i-1}E_2 = 0$, for $i \in \{1, \ldots, 2n_2 - 1\}$. This is equivalent to $\Delta_{M_1}^{(2n_2-1)}A_1 = \Delta_{M_1}^{(2n_2-1)}E_1$, and $\Delta_{M_1}^{(2n_2-1)}E_1 = 0$, or $\Delta_{M_1}^{(2n_2-1)}(A_1 - E_1) = 0$ and $\Delta_{M_1}^{(2n_2-1)}E_1 = 0$. Since M_1 is minimal, by Lemma 4 and Corollary 3, $\operatorname{rank}(\Delta_{M_1}^{(2n_2-1)}) = \operatorname{rank}(\Delta_{M_1}) = n_1 =$ number of columns of $\Delta_{M_1}^{(2n_2-1)}$. Therefore, $E_1 = A_1$ and $E_2 = 0$. Consequently, any matrix A with the same first n_1 rows as A_2 satisfies $C_2A_2^i = C_2A^i$, for $i = 0, 1, \ldots, 2n_2 - 2$, and those matrices A are the only ones that satisfy condition 2. Because the last n_2-n_1 rows of A can be arbitrarily chosen, and A has n_2 columns, one gets that there are $q^{n_2(n_2-n_1)}$ matrices A that satisfy the required conditions. Since $n_1 = \operatorname{rank}(\Delta_{M_1}) = \operatorname{rank}(\Delta_{M_2})$ (because M_1 is minimal, and $M_1 \sim M_2$), the result follows. □

Now, for each matrix A such that $\hat{\Delta}_{M_2} = \hat{\Delta}_M$, *i.e.*, $C_2A_2^i = C_2A^i$, for $i = 0, 1, \ldots, 2n_2 - 1$, one wants to count the number of matrices B that satisfy $\hat{\Delta}_M B_2 = \hat{\Delta}_M B$, that is, satisfy $C_2A^iB_2 = C_2A^iB$, for $i = 0, 1, \ldots, 2n_2 - 1$.

Theorem 9. *Let M_1 be a minimal LFT with structural matrices A_1, B_1, C_1, D_1, and structural parameters l, m, n_1. Let M_2 be the LFT described in Proposition 2. Given a matrix A such that $\hat{\Delta}_{M_2} = \hat{\Delta}_M$, there are exactly $q^{l\left(n_2-\operatorname{rank}(\Delta_{M_2})\right)}$ matrices $B \in \mathcal{M}_{n_2\times l}(\mathbb{F}_q)$ such that $C_2A^iB_2 = C_2A^iB$ for $i = 0, 1, \cdots, 2n_2 - 1$.*

Proof. Let A be a matrix such that $\hat{\Delta}_{M_2} = \hat{\Delta}_M$, and B such that $\hat{\Delta}_M B_2 = \hat{\Delta}_M B$. Then, $\hat{\Delta}_{M_2} B_2 = \hat{\Delta}_{M_2} B$. Consequently, $\Delta_{M_2} B_2 = \Delta_{M_2} B$, which is equivalent to

$\Delta_{M_2}(B_2 - B) = 0$. Since B has n_2 rows, one concludes that there are exactly $n_2 - \text{rank}(\Delta_{M_2})$ rows in B whose entries can be arbitrarily chosen to have a solution of $\Delta_{M_2}(B_2 - B) = 0$. Therefore, and since B has l columns, there are $q^{l\left(n_2 - \text{rank}(\Delta_{M_2})\right)}$ matrices B that satisfy condition 2 of Theorem 4. □

From this one concludes that the number of transducers in $\mathcal{L}_{n_2}$ that are equivalent to M_2 and that have the same augmented diagnostic matrix is $q^{(n_2+l)(n_2-r)}$, where $r = \text{rank}(\hat{\Delta}_{M_2})$, which proves item 2. Item 3 is covered by the following two results together with Corollary 5.

Theorem 10. *Let $A \in \mathcal{M}_{m\times n}(\mathbb{F}_q)$ such that $\text{rank}(A) \neq n$. Then, the number of matrices $X \in GL_n(\mathbb{F}_q)$ such that $AX = A$ is $(q^n - q^{\text{rank}(A)})(q^n - q^{\text{rank}(A)+1}) \cdots (q^n - q^{n-1})$. If $\text{rank}(A) = n$, only the identity matrix satisfies this condition.*

Proof. Let $X \in GL_n(\mathbb{F}_q)$ be such that $AX = A$. Then, there are $n - \text{rank}(A)$ rows in X whose entries can be arbitrarily chosen to have a solution of $AX = A$. But, since X has to be invertible, one has $q^n - q^{\text{rank}(A)}$ possibilities for the "first" of those rows, $q^n - q^{\text{rank}(A)+1}$ for the "second", $q^n - q^{\text{rank}(A)+2}$ for the "third", and so on. Therefore, there are $(q^n - q^{\text{rank}(A)})(q^n - q^{\text{rank}(A)+1}) \cdots (q^n - q^{n-1})$ matrices X that satisfy the required condition. □

The following result is a direct consequence of the previous Theorem and the size of $GL_n(\mathbb{F}_q)$.

Corollary 8. *Let $A \in \mathcal{M}_{m\times n}(\mathbb{F}_q)$. Then, the number of matrices of the form AX, where $X \in GL_n(\mathbb{F}_q)$ is $(q^n - 1)(q^n - q) \cdots (q^n - q^{\text{rank}(A)-1})$.*

Since augmented diagnostic matrices of *LFTs* in the same equivalence class have the same rank, Theorem 6 can be generalized to:

Corollary 9. *Let M be a LFT with structural parameters l,m,n. Then*

$$|[M]_{\sim_n}| = (q^n - 1)\,(q^n - q) \cdots \left(q^n - q^{r-1}\right) q^{(n+l)(n-r)}, \text{ where } r = \text{rank}\,(\Delta_M)\,.$$

Given the structural matrices of a LFT, the last Corollary gives a formula to compute the number of equivalent LFTs with the same size.

6 Conclusion

We presented a way to compute the number of equivalent LFTs with the same size, by introducing a canonial form for LFTs and a method to test LFTs equivalence. This is essencial to have a LFT uniform random generator, and to get an approximate value for the number of non-equivalent injective LFTs, which is indispensable to evaluate the key space of the FAPKC systems.

In future work we plan to use the results in the last section to deduced a recurrence relation that gives the number of non-equivalent LFTs of a given size. This, together with the approximate value for the number of non-equivalent injective LFTs, will allow us to verify if random generation of LFTs is a feasible option to generate keys.

Acknowledgements. This work was partially funded by the European Regional Development Fund through the programme COMPETE and by the Portuguese Government through the FCT under projects PEst-C/MAT/UI0144/2013 and FCOMP-01-0124-FEDER-020486.

Ivone Amorim is funded by FCT grant SFRH/BD/84901/2012.

The authors gratefully acknowledge the useful suggestions and comments of the anonymous referees.

References

1. Amorim, I., Machiavelo, A., Reis, R.: On the invertibility of finite linear transducers. RAIRO - Theoretical Informatics and Applications 48, 107–125 (2014)
2. Bao, F., Igarashi, Y.: Break Finite Automata Public Key Cryptosystem. In: Fülöp, Z. (ed.) ICALP 1995. LNCS, vol. 944, pp. 147–158. Springer, Heidelberg (1995)
3. Dai, Z., Ye, D., Ou, H.: Self-Injective Rings and Linear (Weak) Inverses of Linear Finite Automata over Rings. Science in China (Series A) 42(2), 140–146 (1999)
4. Roche, E., Shabes, Y. (eds.): Finite-State Language Processing. MIT Press, Cambridge (1997)
5. Tao, R.: Invertible Linear Finite Automata. Scientia Sinica XVI(4), 565–581 (1973)
6. Tao, R.: Invertibility of Linear Finite Automata Over a Ring. In: Lepistö, T., Salomaa, A. (eds.) ICALP 1988. LNCS, vol. 317, pp. 489–501. Springer, Heidelberg (1988)
7. Tao, R.: Finite Automata and Application to Cryptography. Springer Publishing Company, Incorporated (2009)
8. Tao, R., Chen, S.: A Finite Automaton Public Key Cryptosystem and Digital Signatures. Chinese Journal of Computers 8(6), 401–409 (1985) (in Chinese)
9. Tao, R., Chen, S.: A Variant of the Public Key Cryptosystem FAPKC3. J. Netw. Comput. Appl. 20, 283–303 (1997)
10. Tao, R., Chen, S.: The Generalization of Public Key Cryptosystem FAPKC4. Chinese Science Bulletin 44(9), 784–790 (1999)
11. Tao, R., Chen, S., Chen, X.: FAPKC3: A New Finite Automaton Public Key Cryptosystem. Journal of Computer Science and Technology 12(4), 289–305 (1997)
12. Dai, Z.-D., Ye, D.F., Lam, K.-Y.: Weak Invertibility of Finite Automata and Cryptanalysis on FAPKC. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 227–241. Springer, Heidelberg (1998)
13. Dai, Z., Ye, D., Ou, H.: Weak Invertibility of Linear Finite Automata I, Classification and Enumeration of Transfer Functions. Science in China (Series A) 39(6), 613–623 (1996)