On Linear Finite Automata and Cryptography

Ivone Amorim, António Machiavelo, Rogério Reis

Technical Report Series: DCC-2011-11

Version 1.0 August 2011

Departamento de Ciência de Computadores

Faculdade de Ciências da Universidade do Porto

Rua do Campo Alegre, 1021/1055,

4169-007 PORTO,

PORTUGAL

Tel: 220 402 900 Fax: 220 402 950

http://www.dcc.fc.up.pt/Pubs/

1 Abstract

Finite automata public-key cryptosystems rely upon characterizations of some types of invertible finite automata, and methods of obtain them as well as their respective inverses. In this paper we provide a much needed clarification of Tao's formalization and basic results on the subject, as well as a new condition for a linear finite automata with memory to be weakly invertible with delay τ. This last result, employing an approach with formal series, uses the Smith's normal form of a polynomial matrix. The proof of the results presented here provides a new way to construct an inverse with delay τ of an invertible linear finite automata.

2 Introduction

In 1985 by R. Tao and S. Chen, in [TC85], introduced a public-key crypto-system based on finite automata. Their basic idea was to use invertible automata for which explicit inverses are known, but such that an inverse of the composition of the two automata was computationally unfeasible to compute. Later on some weakness where found on this system, and some slightly more sofisticated ones were proposed [TC86, Gao94, BI95, RT97, TC97]. These systems are ultimately based on some results used to characterize invertible linear finite automata, and, specially, some techniques to compute an invertible linear automata together with one of its inverses [Tao73]. These techniques were then extended to some other kinds of automata [CT92, TC95, TC00].

In this report, after introducing the basic concepts about finite automata, we describe the several types of invertible automata studied by R. Tao. We then focus our attention on linear automata, and we use formal power series to characterize invertible linear finite automata.

3 Basic concepts on automata and invertible automata

As usual, for a finite set X, we denote by X^n the set of words of length n, with $n \in \mathbb{N}_0$, and $X^0 = \{\varepsilon\}$, where ε denotes the empty word. We will also use $X^* = \cup_{n\geq 0} X^n$, the set of all finite words, and X^ω will denote the set of infinite words.

Definition 3.1. *A* finite automata *is a quintuple* $\langle X, Y, S, \delta, \lambda\rangle$*, where:*

- X *is a nonempty finite set called the* input alphabet *of the finite automaton;*

- Y *is a nonempty finite set called the* output alphabet *of the finite automaton;*
- S *is a nonempty finite set called the* set of states *of the finite automaton;*
- δ *is a function from* $S \times X$ *to* S *called the* state transition function *of the finite automaton;*
- λ *is a function from* $S \times X$ *to* Y *called the* output function.

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

$$\begin{aligned} \delta(s, \varepsilon) &= s \\ \delta(s, x_0 x_1 \dots x_n) &= \delta(\delta(s, x_0), x_1 x_2 \dots x_n) \\ \lambda(s, \varepsilon) &= \varepsilon \\ \lambda(s, x_0 x_1 \dots x_n) &= \lambda(\delta(s, x_0), x_1 x_2 \dots x_n), \end{aligned}$$

where $s \in S, n \in \mathbb{N}$ and $x_0 x_1 \cdots x_n \in X^{n+1}$. In an analogous way, λ may be extended to X^ω. From these definitions it follows that one has, for all $s \in S, \alpha \in X^*$, and for all $\beta \in X^* \cup X^\omega$,

$$\lambda(s, \alpha\beta) = \lambda(s, \alpha)\, \lambda(\delta(s, \alpha), \beta). \tag{1}$$

An important class of finite automata, providing an infinite number of examples, is given by the following:

Definition 3.2. *Let* $f : X^{h+1} \times Y^k \longrightarrow Y$*, with* $h, k \in \mathbb{N}$*, and* X, Y *two nonempty finite sets. The* finite automaton with (h,k)-order memory determined by f *is the automaton* $M_f = \langle X, Y, X^h \times Y^k, \delta_f, \lambda_f \rangle$ *defined by:*

$$\begin{aligned} \lambda_f(< x_1 x_2 \dots x_h, y_1 y_2 \dots y_k >, x) &= f(x_1 x_2 \dots x_h x, y_1 y_2 \dots y_k) =: y, \\ \delta_f(< x_1 x_2 \dots x_h, y_1 y_2 \dots y_k >, x) &= < x_2 \dots x_h x, y_2 \dots y_k y >, \end{aligned}$$

for all $y_1 \dots y_k \in Y^k$ *and* $x_0 x_1 \dots x_h x \in X^{h+1}$*. When* $k = 0$*,* M_f *is called the* finite automaton with h-order input memory determined by f*. When* $h = 0$*,* M_f *is called the* finite automaton with k-order output memory determined by f*. And, we will say that a finite automaton* M *is a* finite automaton with (h,k)-order memory *if* $M = M_f$ *for some function* $f : X^{h+1} \times Y^k \longrightarrow Y$*.*

A central notion, essential for cryptographic purposes, is the notion of invertibility. We start with a concept related to the determination of the inputs by the outputs.

Definition 3.3. *A finite automaton $M = \langle X, Y, S, \delta, \lambda \rangle$ is said to be* invertible with delay τ*, where $\tau \in \mathbb{N}_0$, if $\forall s, s' \in S,\ \forall x, x' \in X,\ \forall \alpha, \alpha' \in X^\tau$,*

$$\lambda(s, x\alpha) = \lambda(s', x'\alpha') \implies x = x'$$

That is, for any $s \in S$ and $\alpha \in X^\tau$, x can be uniquely determined by $\lambda(s, x\alpha)$.

Invertible automata should have inverses of some sort. The following definition introduces the apropriate concept, that we will see is closely related to the previous one.

Definition 3.4. *Let $M = \langle X, Y, S, \delta, \lambda \rangle$, $M' = \langle Y, X, S', \delta', \lambda' \rangle$ be two finite automata. A pair of states $(s', s) \in S' \times S$ is said to be a* match pair with delay τ *if the following condition holds*

$$\forall \alpha \in X^\omega,\ \exists \gamma \in X^\tau :\ \lambda'(s', \lambda(s, \alpha)) = \gamma\alpha\,.$$

Remark: In the previous definition one may replace X^ω by X^*, but then one must take into account that on the right one only gets the first $|\alpha| - \tau$ characters of α.

Proposition 3.5. *If (s', s) is a match pair with delay τ and $\beta = \lambda(s, \alpha)$ for some $\alpha \in X^*$, then $(\delta'(s', \beta), \delta(s, \alpha))$ is also a match pair with delay τ.*

Proof. Assume that (s', s) is a match pair with delay τ, and let $\beta = \lambda(s, \alpha)$ for some $\alpha \in X^*$. Let $\alpha' \in X^\omega$. By (1), one has:

$$\begin{aligned} \lambda'\left(s', \lambda(s, \alpha\alpha')\right) &= \lambda'\left(s', \beta\ \lambda(\delta(s, \alpha), \alpha')\right) \\ &= \lambda'(s', \beta)\ \lambda'(\delta(s', \beta), \lambda(\delta(s, \alpha), \alpha')). \end{aligned}$$

Since (s', s) is a match pair with delay τ, $\exists \alpha_1 \in X^\tau$ such that $\lambda'(s', \lambda(s, \alpha\alpha')) = \alpha_1\alpha\alpha'$. Therefore, $\alpha_1\alpha\alpha' = \gamma\alpha'$, where $\gamma \in X^{\tau+|\alpha|}$.
But, $\lambda'(s', \beta) \in X^{|\alpha|}$. So, $\lambda'(\delta(s', \lambda(s, \alpha), \lambda(\delta(s, \alpha), \alpha')) = \phi\alpha'$, for some $\phi \in X^\tau$. That is, $(\delta(s', \beta), \delta(s, \alpha))$ is a match pair with delay τ. □

Definition 3.6. *M' is called an* inverse with delay τ *of M, if $\forall s \in S$ and $\forall s' \in S'$, (s', s) is a match pair with delay τ. M' is called an* inverse with delay τ*, if M' is an inverse with delay τ of some finite automaton. M' is called an* inverse*, if M' is an inverse with delay τ, for some τ.*

Part of the important role of the automata determined by a function as defined above, in definition 3.2, is revealed by the following result.

Theorem 3.7. *If M is invertible with delay τ, then there exists a finite automaton with τ-order input memory M_f that is an inverse with delay τ of M.*

Proof. Suppose that $M = \langle X, Y, S, \delta, \lambda\rangle$ is invertible automaton with delay τ. Then $\forall s \in S, \forall x \in X, \forall \alpha \in X^\tau$, x can be uniquely determined by the value of $\lambda(s, x\alpha)$. Let $f : Y^{\tau+1} \longrightarrow X$ be the function defined in the following way: if $\exists s \in S, \exists x \in X, \exists \alpha \in X^\tau : \ y_0 y_1 \dots y_\tau = \lambda(s, x\alpha)$, then f is defined at $y_0 y_1 \dots y_\tau$ by $f(y_0 y_1 \dots y_\tau) = x$; otherwise one defines f arbitrarily. Let $M_f = \langle Y, X, Y^\tau, \delta_f, \lambda_f\rangle$ be the finite automaton with τ-order input memory determined by f. To prove the claimed result, one must show that, for all $y_1 \dots y_\tau \in Y^\tau$, for all $s \in S$ and for all $\alpha = x_0 x_1 x_1 \dots \in X^\omega$, there exists an $\gamma \in X^\tau$, such that

$$\lambda_f(y_1 \dots y_\tau, \lambda(s, \alpha)) = \gamma\alpha.$$

Putting:

$$\begin{aligned}
s_0 &= s, \qquad s_{i+1} = \delta(s_i, x_i),\\
z_i &= \lambda(s_i, x_i),\\
\alpha_i &= x_i x_{i+1} x_{i+2} \dots\\
x'_i &= f(y_i \dots y_\tau z_0 \dots z_{i-1})\\
\gamma &= x'_1 x'_2 \dots x'_\tau,
\end{aligned}$$

one has that $\lambda(s, \alpha) = z_0 z_1 z_2 \dots$, and (1) yields

$$\begin{aligned}
\lambda_f(y_1 \dots y_\tau, \lambda(s, \alpha)) &= \lambda_f(y_1 \dots y_\tau, z_0)\ \lambda_f(y_2 \dots y_\tau z_0, \lambda(s_1, \alpha_1))\\
&= x'_1\ \lambda_f(y_2 \dots y_\tau z_0, \lambda(s_1, \alpha_1))\\
&= x'_1 x'_2\ \lambda_f(y_3 \dots y_\tau z_0 z_1, \lambda(s_2, \alpha_2))\\
&= \dots\\
&= x'_1 x'_2 \dots x'_\tau\ \lambda_f(z_0 z_1 \dots z_{\tau-1}, \lambda(s_\tau, \alpha_\tau))\\
&= \gamma\ \lambda_f(z_0 z_1 \dots z_{\tau-1}, z_\tau)\lambda_f(z_1 z_1 \dots z_\tau, \lambda(s_{\tau+1}, \alpha_{\tau+1}))\\
&= \dots\\
&= \gamma\ f(z_0 z_1 \dots z_{\tau-1} z_\tau) f(z_1 z_2 \dots z_\tau z_{\tau+1}) \dots
\end{aligned}$$

But $z_i z_{i+1} \dots z_{i+\tau} = \lambda(s_i, x_i x_{i+1} \dots x_{i+\tau})$, and therefore it follows from the definition of f that $f(z_i z_{i+1} \dots z_{i+\tau}) = x_i$, which finishes the proof. □

It immediately follows that

Corollary 3.8. *M is invertible with delay τ if and only if there exists a finite automaton M' such that M' is an inverse with delay τ of M.*

A weaker form of invertibility is described in the following definition.

Definition 3.9. *A finite automaton $M = \langle X, Y, S, \delta, \lambda \rangle$ is said to be* weakly invertible with delay *τ, with $\tau \in \mathbb{N}_0$, if*

$$\forall s \in S,\ \forall x_0 \dots x_\tau, x'_0 \dots x_\tau \in X^{\tau+1},\ \lambda(s, x_0 \dots x_\tau) = \lambda(s, x'_0 \dots x'_\tau) \implies x_0 = x'_0.$$

That is, for any $s \in S$, and any $x_i \in X$, with $i \in \{0, 1, \dots, \tau\}$, x_0 can be uniquely determined by s and $\lambda(s, x_0 x_1 \dots x_\tau)$.

Definition 3.10. *Let $M =< X, Y, S, \delta, \lambda >$ and $M' =< X, Y, S', \delta', \lambda' >$ be two finite automata. M' is called a* weak inverse with delay *τ of M, if $\forall s \in S$, $\exists s' \in S$ such that (s', s) is a match pair with delay τ. M' is called a* weak inverse with delay *τ, if M' is a weak inverse with delay τ of some finite automaton. M' is called a* weak inverse, *if M' is a weak inverse with delay τ for some τ.*

For weakly invertible automata a result entirely similar to theorem 3.7 and its corollary can be stated. In particular, one has:

Theorem 3.11. *M is weakly invertible with delay τ if and only if there exists a finite automaton M' such that M' is a weak inverse with delay τ of M.*

Proof. See [Tao09]. □

4 Invertibility with delay τ of linear finite automata

Definition 4.1. *If X, Y and S are vector spaces over a field $\mathbb{F}$, then a finite automaton $M = \langle X, Y, S, \delta, \lambda \rangle$ is said to be* linear *over $\mathbb{F}$ when both $\delta : S \times X \to S$ and $\lambda : S \times X \to Y$ are linear maps.*

If X, Y and S have dimensions l, m and n, respectively, then

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

for some $n \times n$ matrix A, $n \times l$ matrix B, $m \times n$ matrix C, and $m \times l$ matrix D, and where $s \in S, x \in X$. The matrices A, B, C, D are called the *structural matrices* of the finite automaton, and l, m, n are called *structural parameters* of the finite automaton.

Let $M = \langle X, Y, S, \delta, \lambda \rangle$ be a linear finite automaton over a finite field $\mathbb{F}$, with structure matrices A, B, C, D. For any $s_0 \in S$ and $x_0 x_1 \cdots \in X^\omega$, let:

$$s_{t+1} = As_t + Bx_t, \quad t = 0, 1, \ldots \tag{2}$$

and

$$y_t = Cs_t + Dx_t, \quad t = 0, 1, \ldots \tag{3}$$

where $A \in \mathcal{M}_{n\times n}$, $B \in \mathcal{M}_{n\times \ell}$, $C \in \mathcal{M}_{m\times n}$, and $D \in \mathcal{M}_{m\times \ell}$.

The following result is presented in [Tao73] without proof, and in [Tao09] with a proof by induction. Here we present a more conceptual proof using formal series, that can be seen as a preliminary to the approach that will be presented in section 5.

Theorem 4.2. *For all $t \geq 0$ one has, for all $s_0 \in S$ and $x_0 x_1 \ldots x_t \in X^{t+1}$,*

$$s_t = A^t s_0 + \sum_{i=0}^{t-1} A^{t-1-i} B x_i, \tag{4}$$

and

$$y_t = CA^t s_0 + \sum_{i=0}^{t} H_{t-i} x_i, \tag{5}$$

where $H_0 = D$, $H_j = CA^{j-1}B$, $j > 0$.

Proof. Multiplying both sides of equation (2) by z^{t+1}, and adding all the equations, for $t \geq 0$, in the ring of formal series $\mathbb{F}[[z]]$, one obtains:

$$\sum_{t\geq 0} s_{t+1} z^{t+1} = \sum_{t\geq 0} As_t z^{t+1} + \sum_{t\geq 0} Bx_t z^{t+1},$$

or

$$\sum_{t\geq 0} s_t z^t - s_0 = z \sum_{t\geq 0} As_t z^t + z \sum_{t\geq 0} Bx_t z^t,$$

which yields

$$(I - Az)S(z) = s_0 + zBX(z),$$

where $S(z) = \sum_{t\geq 0} s_t z^t$, and $X(z) = \sum_{t\geq 0} x_t z^t$.

Since $1 - Az$ is invertible in $\mathbb{F}[[z]]$, and $(1 - Az)^{-1} = \sum_{n\geq 0} A^n z^n$, one gets:

$$S(z) = \sum_{n\geq 0} A^n s_0 z^n + \sum_{n\geq 0} A^n BX(z)z^{n+1},$$

which gives (4).

Now, if one multiplies both sides of equation (3) by z^t, and adds all the equations, for $t \geq 0$, in the ring of formal series $\mathbb{F}[[z]]$, one obtains:

$$Y(z) = C\,S(z) + D\,X(z).$$

Substituing $S(z)$ on this equation, one gets:

$$Y(z) = C\left(\sum_{n\geq 0} A^n s_0 z^n + \sum_{n\geq 0} A^n BX(z)z^{n+1}\right) + DX(z),$$

which is equivalent to:

$$Y(z) = C\sum_{n\geq 0} A^n s_0 z^n + \left(C\sum_{n\geq 0} A^n Bz^{n+1} + D\right) X(z).$$

This proves the validity of (5). □

We can rewrite equation (5) as:

$$Y_t = G_t V_t,$$

where, using A^T to denote the transpose of a matrix A,

$$Y_t = [y_t, \ldots, y_1, y_0]^T, \qquad V_t = [x_t, \ldots, x_0, s_0]^T$$

and

$$G_t = \begin{bmatrix} H_0 & H_1 & \cdots & H_{t-1} & H_t & CA^t \\ 0 & H_0 & \cdots & H_{t-2} & H_{t-1} & CA^{t-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & H_0 & H_1 & CA \\ 0 & 0 & \cdots & 0 & H_0 & C \end{bmatrix}.$$

Set $J_t = [H_t\, H_{t-1}\, \cdots\, H_0]^T$, and set

$$K_t = \begin{bmatrix} H_0 & H_1 & \cdots & H_{t-1} & CA^t \\ 0 & H_0 & \cdots & H_{t-2} & CA^{t-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & H_0 & CA \\ 0 & 0 & \cdots & 0 & C \end{bmatrix}.$$

The following result gives a condition for a linear finite automaton to be invertible with delay $\tau \in \mathbb{N}_0$. This result appears in [Tao73, Tao09], without proof.

Theorem 4.3. *M is invertible with delay τ if and only if*

$$rank(G_\tau) = rank(K_\tau) + \ell.$$

Proof. In what follows, we will denote the space generated by the columns of a matrix A by $< A >$. The present result can be shown by proving the following equivalences:

$$\begin{aligned} M \text{ invertible with delay } \tau \quad &\underset{(A)}{\iff} \quad \forall V_\tau \in X^{\tau+1} \times S \quad G_\tau V_\tau = 0 \implies x_0 = 0 \\ &\underset{(B)}{\iff} \quad dim(< J_\tau >) = \ell \quad \wedge \quad < J_\tau > \cap < K_\tau >= 0 \\ &\underset{(C)}{\iff} \quad rank(G_\tau) = rank(K_\tau) + \ell. \end{aligned}$$

The first equivalence is immediate from definition 3.3, and the fact that here $\lambda(s_0, x_0 x_1 \dots x_t)$ is essentially equal to $G_t V_t$.

Now, let us prove the only if part of equivalence (B). Assume that $G_\tau V_\tau = 0$, and that $dim(< J_\tau >) = \ell$ and $< J_\tau > \cap < K_\tau >= 0$. One has,

$$G_\tau V_\tau = 0 \iff K_\tau \left[x_\tau\, x_{\tau-1}\, \cdots\, x_1\, s_0\right]^T = -J_\tau \left[x_0\right],$$

Since, $< J_\tau > \cap < K_\tau >= 0$, that gives:

$$K_\tau \left[x_\tau\, x_{\tau-1}\, \cdots\, x_1\, s_0\right]^T = 0 \quad \wedge \quad J_\tau \left[x_0\right] = 0,$$

and from $dim(< J_\tau >) = \ell$, one obtains $x_0 = 0$.

To prove the if part of equivalence (B), one proves that

$$dim(< J_\tau >) \neq \ell \quad \vee \quad < J_\tau > \cap < K_\tau >\neq 0 \implies \exists V_\tau\; G_\tau V_\tau = 0 \wedge x_0 \neq 0.$$

First, let us assume that $dim(< J_\tau >) \neq \ell$, that is,

$$\exists\, x_0 \neq 0 :\; J_\tau[x_0] = 0.$$

This implies

$$\exists\, V_\tau = [0\ \cdots\ 0\ x_0\ 0]^T :\ G_\tau V_\tau = 0 \wedge x_0 \neq 0.$$

Now, let us assume that $< J_\tau > \cap < K_\tau > \neq 0$. This implies that

$$\exists\, [x_t\ \cdots\ x_1\ s_0]^T \neq 0, x_0 \neq 0 :\ K_\tau [x_t\ \cdots\ x_1\ s_0]^T = J_\tau x_0$$

which yields $V_\tau = [x_t\ \cdots\ x_1\ (-x_0)\ s_0]^T$ with $G_\tau V_\tau = 0 \wedge x_0 \neq 0$.

To prove the only if part of the last equivalence, suppose that $rank(G_\tau) = \ell + rank(K_\tau)$. Since $< G_\tau > = < J_\tau > \cup < K_\tau >$, and $J_\tau \in \mathcal{M}_{m(\tau+1)\times l}$, one has $rank(J_\tau) = \ell$. Consequently, $< J_\tau > \cap < K_\tau > = 0$.

Finally, to deal with the if part of the last equivalence, assume that one has $dim(< J_\tau >) = \ell$, $< J_\tau > \cap < K_\tau > = 0$, and that $< G_\tau > = < J_\tau > \cup < K_\tau >$. Then,

$$dim(< G_\tau >) = dim(< J_\tau >) + dim(< K_\tau >),$$

and therefore,

$$rank(G_\tau) = \ell + rank(K_\tau).$$

□

There is an analogous condition for a linear finite automaton to be weakly invertible with delay τ. Let, $X_t = [x_t\ x_{t-1}\ \cdots\ x_0]^T$,

$$K'_t = \begin{bmatrix} H_0 & H_1 & \cdots & H_{t-1} \\ 0 & H_0 & \cdots & H_{t-2} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & H_0 \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \text{ and } G'_t = \begin{bmatrix} H_0 & H_1 & \cdots & H_{t-1} & H_t \\ 0 & H_0 & \cdots & H_{t-2} & H_{t-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & H_0 & H_1 \\ 0 & 0 & \cdots & 0 & H_0 \end{bmatrix}.$$

One then has

Theorem 4.4. *M is weakly invertible with delay τ if and only if*

$$rank(G'_\tau) = rank(K'_\tau) + \ell.$$

5 An approach envolving formal series

Let M be a linear finite automata over a unitary ring R defined by:

$$y_{t+\tau} = \sum_{i=0}^{\tau-1} a_i\, y_{t+i} + \sum_{j=0}^{\tau} b_j\, x_{t+j} \quad (t \geq 0) \tag{6}$$

where $a_i, b_j \in R$, for $i \in \{0, \cdots, \tau-1\}$ and $j \in \{0, \cdots, \tau\}$.

If one multiplies (6) by $z^{t+\tau}$, and adds all the equations, for $t \geq 0$, in the ring of formal series $R[[z]]$, one obtains:

$$\begin{aligned}
\sum_{t\geq 0} y_{t+\tau}\, z^{t+\tau} &= \sum_{t\geq 0} \left(\sum_{i=0}^{\tau-1} a_i\, y_{t+i} + \sum_{j=0}^{\tau} b_j\, x_{t+j} \right) z^{t+\tau} \\
&= \sum_{i=0}^{\tau-1} a_i \sum_{t\geq 0} y_{t+i}\, z^{t+\tau} + \sum_{j=0}^{\tau} b_j \sum_{t\geq 0} x_{t+j}\, z^{t+\tau} \\
&= \sum_{i=0}^{\tau-1} a_i\, z^{\tau-i} \sum_{t\geq 0} y_{t+i}\, z^{t+i} + \sum_{j=0}^{\tau} b_j\, z^{\tau-j} \sum_{t\geq 0} x_{t+j}\, z^{t+j}
\end{aligned}$$

Then,

$$\begin{aligned}
&\sum_{t\geq 0} y_t\, z^t - \sum_{k=0}^{\tau-1} y_k\, z^k = \\
&\quad = \sum_{i=0}^{\tau-1} a_i\, z^{\tau-i} \left(\sum_{t\geq 0} y_t\, z^t - \sum_{k=0}^{i-1} y_k\, z^k \right) + \sum_{j=0}^{\tau} b_j\, z^{\tau-j} \left(\sum_{t\geq 0} x_t\, z^t - \sum_{k=0}^{j-1} x_k\, z^k \right).
\end{aligned}$$

Letting,

$$f(z) = 1 - \sum_{i=0}^{\tau-1} a_i\, z^{\tau-i}, \quad Y(z) = \textstyle\sum_{t\geq 0} y_t\, z^t,$$

$$g(z) = \sum_{j=0}^{\tau} b_j\, z^{\tau-j}, \quad X(z) = \textstyle\sum_{t\geq 0} x_t\, z^t,$$

$$r(z) = \sum_{k=0}^{\tau-1} y_k\, z^k - \sum_{i=0}^{\tau-1} a_i\, z^{\tau-i} \left(\sum_{k=0}^{i-1} y_k\, z^k \right) - \sum_{j=0}^{\tau} b_j\, z^{\tau-j} \left(\sum_{k=0}^{j-1} x_k\, z^k \right),$$

we can rewrite the equality above as follows:

$$f(z)Y(z) - g(z)X(z) = r(z). \tag{7}$$

Note that $f(0) = 1$, and that the polynomial $r(z)$ depends on the initial state of the automaton (cf. definition 3.2).

Remark: It is easy to see that, conversely, an equation of this form defines a linear automaton, for any $f(z), g(z) \in R[z]$ with $f(0) = 1$, and where $r(z)$ denotes a polynomial which varies with the initial values of the input and of the output, and whose degree is less than the maximum of the degrees of f and g.

Theorem 5.1. *Let R be an unitary ring. A linear automaton given by $fY - gX = r$ with $f, g, r \in R[z]$ and $f(0) = 1$ satisfies an equation of the form $aY - z^\tau X = b$, for some $a, b \in R[z]$, if and only if*

$$\exists\, h \in R[z] :\ hg = z^\tau. \tag{8}$$

Proof. The if part is straightforward: one just needs to take $a = hf$ and $b = hr$. To prove the only if part, assume that an automaton given by $fY - gX = r$ with $f, g, r \in R[z]$ and $f(0) = 1$ satisfies an equation of the form $aY - z^\tau X = b$, for some $a, b \in R[z]$.
Since $f(0) = 1$, f has an inverse, $f^{-1} \in R[[z]]$, and from $fY - gX = r$ one obtains $Y = f^{-1}r + f^{-1}gX$. Substituing in the second equation, one gets:

$$(af^{-1}g - z^\tau)X = b - af^{-1}r.$$

Since one may freely choose the initial state and the input sequence, taking the initial state as being $\mathbf{0}$, and a non-zero input sequence $X = \sum_{t \geq \tau} x_t\, z^t$, one obtains

$$(af^{-1}g - z^\tau)X = 0.$$

Consequently,

$$af^{-1}g = z^\tau.$$

It then follows that $af^{-1}r = b$, which means that

$$af^{-1}r \in R[z],$$

for all possible polynomials $r(z)$. Choosing, as we may, the initial values such that $y_{\tau-1} = 1$ and all other zero, so that $r(z) = z^{\tau-1}$, one sees that one must have $af^{-1} \in R[z]$. Therefore,

$$\exists\, h \in R[z] :\ hg = z^\tau,$$

which finishes the proof. □

In what follows, we denote by $\mathcal{M}(R)$ the set of all matrices, of any dimensions, over the ring R.

Lema 5.2. *Let $\mathbb{F}$ be a field, and $G \in \mathcal{M}(\mathbb{F}[z])$. Then,*

$$\exists\, H \in \mathcal{M}(\mathbb{F}[z]) :\ HG = z^\tau I \iff d \mid z^\tau,$$

where d is the elementary divisor with the highest degree of G in Smith's normal form[1]*, and I is the appropriate identity matrix.*

Proof. Let $G \in \mathcal{M}(\mathbb{F}[z])$. Since $\mathbb{F}[z]$ is a principal ideal domain, there exist $U, V \in \mathcal{M}(\mathbb{F}[z])$, matrices with the appropriate dimensions, such that $D = UGV$ is the Smith's normal form of G. One then has,

$$\begin{aligned}
\exists\, H \in \mathcal{M}(\mathbb{F}[z]) :\ HG = z^\tau I \quad &\iff \quad \exists\, H \in \mathcal{M}(\mathbb{F}[z]) :\ HU^{-1}UGV = z^\tau V \\
&\iff \quad \exists\, H \in \mathcal{M}(\mathbb{F}[z]) :\ HU^{-1}D = Vz^\tau \\
&\iff \quad \exists\, H \in \mathcal{M}(\mathbb{F}[z]) :\ V^{-1}HU^{-1}D = z^\tau \\
&\iff \quad \exists\, H = (h_{ij})_{i,j} \in \mathcal{M}(\mathbb{F}[z]) :\ HD = z^\tau \\
&\iff \quad \forall_{i,j}\, \exists\, h_{i,j} \in \mathbb{F}[z] :\ \begin{cases} h_{ij} = 0, & \text{if } i \neq j \\ h_{ii}d_i = z^\tau, & \end{cases} \\
&\iff \quad d \mid z^\tau,
\end{aligned}$$

where d_i are the elementary divisors of G, and d is the one with the highest degree. □

Since a matrix polynomial $g \in \mathcal{M}(\mathbb{F})[z]$ is essentially the same thing as a polynomial matrix, from the above results one gets:

Theorem 5.3. *Let $\mathbb{F}$ be a field. An automaton given by $fY - gX = r$ with $f, g, r \in \mathbb{F}[z]$ and $f(0) = 1$ satisfies an equation of the form $aY - z^\tau X = b$, for some $a, b \in \mathbb{F}[z]$, if and only if*

$$d \mid z^\tau, \tag{9}$$

where d is the elementary divisor with the highest degree of G, and G is the polynomial matrix that corresponds to g.

Corollary 5.4. *Let M be an automaton given by the equation $fY - gX = r$ with $f, g, r \in \mathbb{F}[z]$ and $f(0) = 1$, where $\mathbb{F}$ is any field. If the greatest elementary divisor of g divides z^τ, for some $\tau \in \mathbb{N}$, then M is weakly invertible with delay τ.*

[1] For more on Smith's normal form, see [New72].

6 Conclusion

The techniques to construct an invertible finite automaton and find one of its inverses have two fundamental applications: they are used to construct the pairs of keys necessary for encryption, decryption and signature, and also can be used to attack the existent cryptographic systems based on finite automata.

The approach presented on section 5 gives a condition to verify if a linear finite automaton with memory is weakly invertible with delay τ, using the Smith's normal form of a polynomial matrix. The results therein shown can also be used to construct an inverse with delay τ of an invertible automaton. Since there are algorithms that compute the Smith's normal form of polynomial matrices on deterministic polynomial time [Vil95], those results seem very promising for cryptographic uses.

References

[BI95] Feng Bao and Yoshihide Igarashi. Break finite automata public key cryptosystem. In *International Congress of Mathematicans*, pages 147–158, 1995.

[CT92] Shihua Chen and Renji Tao. Invertibility of quasi-linear finite automata. *Advances in Cryptology - CHI - NACRYPT'92*, pages 77–86, 1992. (in Chinese).

[Gao94] Xiang Gao. *Finite automaton public key cryptosystems and digital signatures-analysis, design and implementation.* PhD thesis, Institute of Software, Chinese Academy of Sciences, Beijing, 1994. (in chinese).

[New72] Morris Newman. *Integral matrices.* Academic Press, 1972.

[RT97] Xuemei Chen Renji Tao, Shihua Chen. FAPKC3: a new finite automaton public key cryptosystem. *Journal of Computer Science and Technology*, 12(4):289–305, 1997.

[Tao73] Renji Tao. Invertible linear finite automata. *Scientia Sinica*, XVI(4):565–581, November 1973.

[Tao09] Renji Tao. *Finite Automata and Application to Cryptography.* Springer Publishing Company, Incorporated, 2009.

[TC85] Renji Tao and Shihua Chen. A finite automaton public key cryptosystem and digital signatures. *Chinese Journal of Computers*, 8(6):401–409, 1985. (in Chinese).

[TC86] Renji Tao and Shihua Chen. Two varieties of finite automaton public key cryptosystem and digital signatures. *Journal of Computer Science and Technology*, 1(1):9–18, 1986.

[TC95] Renji Tao and Shihua Chen. Generating a kind of nonlinear finite automata with invertibility by transfomation method. Technical Report No. ISCAS-LCS-95-05, Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, June 1995.

[TC97] Renji Tao and Shihua Chen. A variant of the public key cryptosystem FAPKC3. *J. Netw. Comput. Appl.*, 20:283–303, July 1997.

[TC00] Renji Tao and Shihua Chen. Constructing finite automata with invertibility by transformation method. *Journal of Computer Science and Technology*, 15:10–26, 2000.

[Vil95] Gilles Villard. Generalized subresultants for computing the smith normal form of polynomial matrices. *J. Symb. Comput.*, 20:269–286, September 1995.