アルゴリズム 42−3
（1994. 11. 18）

弱可逆有限オートマトンの分解に関するいくつかの結果

鮑豊　五十嵐善英　于小梅
群馬大学工学部情報工学科

概要

本論文で取り扱う弱可逆性有限オートマトン (WIFA と略記する) は入力系列を同じ長さの出力系列に変換する変換器である。長さ $\tau+1$ の入力系列の最初の文字が出力系列と初期状態から一意に決るとき、その変換器を遅れ τ の WIFA という。入力アルファベットと出力アルファベットが同じで、その大きさが n である変換器を n−WIFA で表す。$n > 1$ のとき、二つの遅れ 1 の n−WIFA に分解できない遅れ 2 の n−WIFA が存在することを示し。任意の素数 p について、遅れ 1 の p−WIFA は遅れ 0 の n−WIFA と単位遅れ回路に分解できることを示す。また 2−WIFA が遅れ 0 の WIFA と k 個の単位遅れ回路に分解できるのは、M の全ての状態が遅れ k を持つとき、かつそのときに限ることを示す。

Some Results on Decomposability of Weakly Invertible Finite Automata

Feng Bao　Yoshihide Igarashi　Xiaomei Yu
Department of Computer Science, Gunma Univercity
Kiryu, 376 Japan
Email: igarashi@cs.gunma-u.ac.jp

abstract

A weakly invertible finite automaton (WIFA for short) is an invertible transducer which converts a finite input string into an output string of the same-length. A finite automaton is called a WIFA *with delay* τ if and only if the first letter of the input string of length $\tau+1$ is uniquely determined by the coorresponding output string and the initial state. The composition of two WIFAs is their natural concatenation, which is again a WIFA whose delay is the sum of the delays of the two WIFAs. Previously, seldom is known about the decomposition of a WIFA into the WIFAs with smaller delay. In this paper We present various results on this subject. The interest of this topic comes from both theory and application aspects. In order to capture the essence of the decompposability problem, we only conc entrate on the WIFAs such that the output alphabet is the same as the input alphabet. We call $M = (X, X, S, \delta, \lambda)$ an n-FA if $|X| = n$. We prove that for any $n > 1$, there exist some n-WIFAs with delay 2 which cannot be decomposed into two n-WIFAs *with delay* 1. and that for any prime number p, every strongly connected p-WIFA *with delay* 1, can be decomposed into a WIFA *with delay* 0 and a *delay unit*. A *delay unit* is a special WIFA *with delay* 1, which is actually a logic memory cell. For any 2-WIFA M, M can be decomposed into a WIFA *with delay* 0 and k connected *delay units* if and only if all the states of M have delay k.

1 Introduction

The concept of invertible finite automata was first proposed by D.A. Huffman as "Information-lossless finite state logical machine" in [8]. Since then, many studies have been done towards this direction [1, 3-7, 9-14, 16, 19]. Among them, in [6], Even used the concept of generalized automata instead of "sequential machine" and "logical machine". In the past two decades, the invertibility of finite automata has been intensively and systematically studied by Tao and Chen [3-5, 12-17]. Reference [12] was the first book in this area in which both invertible and weakly invertible finite automata were investigated.

Formally speaking, a finite automaton is a five-tuple $M = (X, Y, S, \delta, \lambda)$, Where

X is a finite input alphabet

Y is a finite output alphabet

S is a finite set of internal states

δ is a next-state function

$$\delta : S \times X \to S$$

λ is an output function

$$\lambda : S \times X \to Y$$

δ can be naturally extended to a mapping from $S \times X^*$ to S as follows, where X^* denotes the set of all the finite strings over X (including the empty string Λ).

For any $s \in S, \alpha \in X^*, x \in X$

$$\delta(s, \Lambda) = s$$

$$\delta(s, \alpha x) = \delta(\delta(s, \alpha), x)$$

Similarly, λ can be naturally extended to a mapping from $S \times (X^* \cup X^w)$ to $Y^* \cup Y^w$, where X^w denotes the set of all the infinite strings over X.

For any $s \in S, \alpha \in X^* \cup X^w, x \in X$

$$\lambda(s, \Lambda) = \Lambda$$

$$\lambda(s, x\alpha) = \lambda(s, x)\lambda(\delta(s, x), \alpha)$$

From the above definition, our finite automaton is a transducer which converts a sequence over the input alphabet into a sequence over the output alphabet rather than just an acceptor.

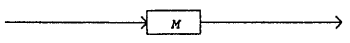

Fig. 1

Definition 1. Let $M = (X, Y, S, \delta, \lambda)$ be a finite automaton. If for any $s \in S$ and $\alpha, \alpha' \in X^w, \lambda(s, \alpha) = \lambda(s, \alpha')$ always implies $\alpha = \alpha'$, then M is said to be weakly invertible, i.e. , M is a WIFA.

A finite automaton $M = (X, Y, S, \delta, \lambda)$ is called an invertible finite automaton (IFA) if for any $\alpha, \alpha' \in X^w$, $s, s' \in S$, $\lambda(s, \alpha) = \lambda(s', \alpha')$ always implies $\alpha = \alpha'$. Apparently , IFA is a special case of a WIFA. In this paper, we only consider WIFA.

The theory of invertibility of finite automata has been extensively applied in cryptography [2, 13, 15, 18]. Besides the regular key cryptosystem proposed in [13], Finite Automaton Public Key Cryptosystem (FAPKC for short) is an almost ten-years' standing public key cryptosystem and digital signature [15]. FAPKC encrypts the plaintext by a WIFA which is composed of a linear WIFA with delay τ and a non-linear WIFA with delay 0. Since it is a stream cipher, FAPKC possesses the advantage of the convenience that the plaintext need not be divided into blocks. And its speed is very fast while its key size remains small [18]. Recently, an identity based public key cryptosystem and signature scheme has been proposed, which was also founded on the theory of WIFA [17]. We foresee that the theory of invertibility of finite automata has great potential in its application to cryptography.

In this paper, we concentrate on the decomposability of WIFAs. Informally speaking, the composition of two WIFAs realizes their concatenation, i.e., the latter takes the former's output as its input. The composition of two WIFAs is again a WIFA, whose delay is the sum of the delays of the two WIFAs. It's very complex and difficult to decide whether a WIFA can be decomposed into two or more WIFAs with smaller delays or to show what kind of WIFAs can be decomposed. Previously, seldom is known about this problem. Its interest comes from two aspects. The theoretical aspect of this problem is to investigate the structure of WIFAs. Generally speaking, WIFAs with smaller delay have simpler structures than WIFAs with larger delay. Another interest in the decomposability of WIFA comes from the cryptographic application. Comprehension of the decomposition of WIFA helps us to study the security of FAPKC and other cryptosystems based on the theory of WIFA. To make this paper self-contained, we first review some basic definitions and properties which can be found in [6, 7, 12].

Definition 2. A finite automaton $M = (X, Y, S, \delta, \lambda)$ is said to be a WIFA with delay τ if for any $s \in S$, $\alpha, \alpha' \in X$ and $\alpha, \alpha' \in X^\tau (\tau$ is a positive integer, X^τ is the set of all the τ-length strings over $X)$, $\lambda(s, a\alpha) = \lambda(s, a'\alpha')$ always implies $a = a'$.

Proposition 1. A finite automaton M is a WIFA if and only if M is a WIFA with delay τ for some $\tau \leq n(n-1)/2$, where n is the number of the states of M.

Definition 3. Let $M = (X, Y, S, \delta, \lambda)$ and $M' = (Y, X, S', \delta', \lambda')$ be a pair of finite automata. If for any $s \in S$ there exists $s' \in S'$ such that for any $\alpha \in X^w$, there exists $\alpha_0 \in X^\tau$ satisfying $\lambda'(s', \lambda(s, \alpha)) = \alpha_0\alpha$, then M' is said to be a weak inverse with delay τ of M.

Proposition 2. M is a WIFA with delay τ if and only if M has a weak inverse with delay τ.

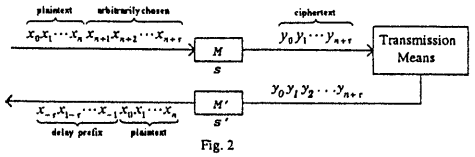

Fig. 2

The state s' in definition 3 is said to be the *match state* of the state s. Fig. 2 shows the principle of the application of WIFA to cryptography.

2 Compositions of Finite Automata

The compositions of WIFAs were first defined and applied in [15]. Formally speaking, the composition of two finite automata $M_1 = (X, Y, S_1, \delta_1, \lambda_1)$ and $M_2 = (Y, Z, S_2, \delta_2, \lambda_2)$ is a new finite automaton

$$C(M_1, M_2) = (X, Z, S_1 \times S_2, \delta, \lambda)$$

Where

$$\delta((s_1, s_2), x) = (\delta_1(s_1, x), \delta_2(s_2, \lambda_1(s_1, x)))$$
$$\lambda((s_1, s_2), x) = \lambda_2(s_2, \lambda_1(s_1, x))$$

for any $(s_1, s_2) \in S_1 \times S_2$, i.e. for any $s_1 \in S_1, s_2 \in S_2$. Fig. 3 shows the composition of M_1 and M_2.

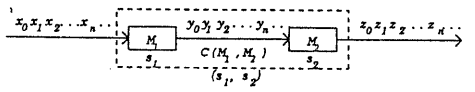

Fig. 3

For the study of the composition of WIFAs, we restrict our concentration on those finite automata where output alphabets are the same as their input alphabets. We say that $M = (X, X, S, \delta, \lambda)$ is a finite automaton over X. For $|X| = n$, we say that M is an n-FA. And for these automata, composition is an operation on finite automata over X.

We denote $C(M_1, M_2)$ by $M_1 \cdot M_2$. Let M_1, M_2, M_3 be finite automata over X. Then, it is not difficult to prove that $(M_1 \cdot M_2) \cdot M_3$ is *isomophic* to $M_1 \cdot (M_2 \cdot M_3)$ [15]. Hence, it is reasonable to denote the composition of M_1, M_2, M_3 by $M_1 \cdot M_2 \cdot M_3$ or just $M_1 M_2 M_3$. For the same reason, the composition of $M_1, M_2, ..., M_k$ (all M_i are over X), is denoted by $M_1 M_2 \cdots M_k$, and its states are in the form $(s_1, s_2, ..., s_k)$ where s_i is a state of M_i.

Definition 4. Let $M_1 = (X, X, S_1, \delta_1, \lambda_1)$ and $M_2 = (X, X, S_2, \delta_2, \lambda_2)$ be two finite automata over X. We say $s_1 \in S_1$ is equivalent to $s_2 \in S_2$, denoted by $s_1 \sim s_2$, if for any $\alpha \in X^w$, $\lambda_1(s_1, \alpha) = \lambda_2(s_2, \alpha)$.

Definition 5. Let M_1 and M_2 be two finite automata over X. M_1 is said to be weaker than M_2, denoted by $M_1 < M_2$, if for any state s_1 of M_1, there is a state s_2 of M_2 such that $s_1 \sim s_2$. If $M_1 < M_2$ and $M_2 < M_1$, we say M_1 and M_2 are equivalent, denoted by $M_1 \sim M_2$.

Let $M_1, M_2, ..., M_k, M_1', M_2', ..., M_k'$ be finite automata over X. The following three theorems are immediate.

Theorem 1. Let s_i be a state of M_i and s_i' be a state of $M_i', i = 1, 2, ..., k$. If $s_i \sim s_i', i = 1, 2, ..., k$, then state $(s_1, s_2, ..., s_k)$ of $M_1 M_2 \cdots M_k$ is equivalent to state $(s_1', s_2', ..., s_k')$ of $M_1' M_2' \cdots M_k'$.

Theorem 2. If $M_i < M_i', i = 1, 2, ..., k$, then $M_1 M_2 \cdots M_k < M_1' M_2' \cdots M_k'$.

Theorem 3. If $M_i \sim M_i', i = 1, 2, ..., k$, then $M_1 M_2 \cdots M_k \sim M_1' M_2' \cdots M_k'$.

Let M_1 and M_2 be two WIFAs over X. It is directly obtained from the definition of WIFA that $M_1 M_2$ is also a WIFA. Specifically, if M_1 is a WIFA with delay τ_1 and M_2 is a WIFA with delay τ_2, then $M_1 M_2$ is a WIFA with delay $\tau_1 + \tau_2$.

Definition 6. Let $M, M_1, M_2, ..., M_k$ be finite automata over X. M is said to be decomposable into $M_1, M_2, ..., M_k$ if $M < M_1 M_2 \cdots M_k$.

The analysis of the structure of WIFA's is one of the main tasks in the theory of WIFAs. The structure of linear WIFAs has been intensively studied in [12]. However, much remains unknown for non-linear case. Decomposing a WIFA into WIFAs with smaller delay is a good approach toward this aim, since WIFAs with smaller delay have comparatively simpler structures. For example, let's consider 2-WIFAs over $X = \{0, 1\}$. Every WIFA with delay 0 over X is in the form shown in Fig.4.

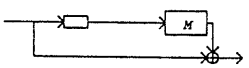

Fig. 4

In Fig.4, $\longrightarrow\square\longrightarrow$ is a delay unit, or say a memory cell in terms of logical net [8], and M is an arbitrary FA over X. Hereafter we call a 2-WIFA also a binary WIFA.

Definition 7. M is said to be a WIFA with exact delay τ if M is a WIFA with delay τ but not a WIFA with delay τ-1.

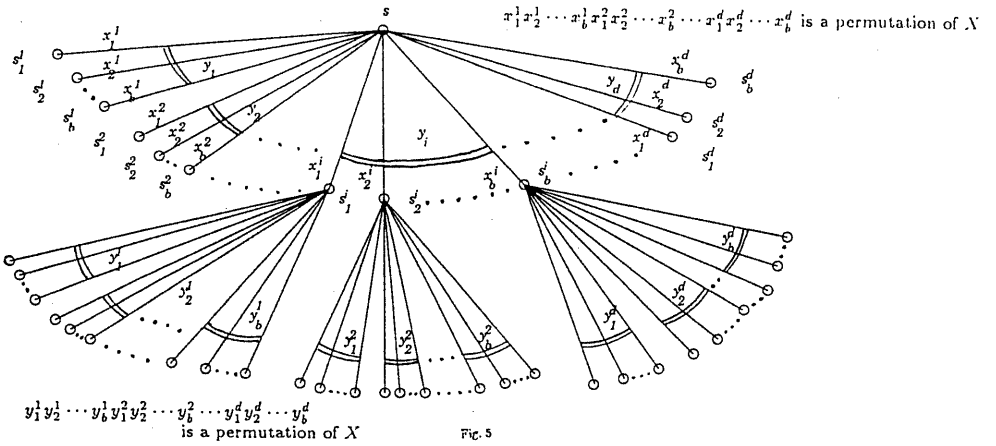

Fig. 5

3 WIFAs with Delay One

We first consider the WIFA with delay one in this section.

First we introduce some notations. Let $M = (X, Y, S, \delta, \lambda)$ be a finite automaton. We define, for $s \in S, y \in Y$,

$Out(s) = \{y \in Y \mid y = \lambda(s, x) \text{ for some } x \in X\}$

$d(s) = \mid Out(s) \mid$, the cardinality of $Out(s)$

$In(s, y) = \{x \in X \mid \lambda(s, x) = y\}$

$St(s) = \{t \in S \mid t = \delta(s, \alpha) \text{ for some } \alpha \in X^*\}$

$St(s, y) = \{t \in S \mid t = \delta(s, x) \text{ and } y = \lambda(s, x) \text{ for some } x \in X\}$.

Lemma 1. $M = (X, Y, S, \delta, \lambda)$ is a WIFA with delay 1. If $x_1 \neq x_2, x_1, x_2 \in X$ and $x_1, x_2 \in In(s, y)$ for some $s \in S, y \in Y$, then $Out(\delta(s, x_1)) \cap Out(\delta(s, x_2)) = \phi$.

Proof. The proof is directly from the definition of WIFAs with delay 1. $x_1, x_2 \in In(s, y)$ means $\lambda(s, x_1) = \lambda(s, x_2) = y$. If $Out(\delta(s, x_1)) \cap Out(\delta(s, x_2)) \neq \phi$, then there exists a $y' \in Y$ such that $y' \in Out(\delta(s, x_1))$ and $y' \in Out(\delta(s, x_2))$. That means $\exists x_1', x_2' \in X$ such that $\lambda(\delta(s, x_1), x_1') = \lambda(\delta(s, x_2), x_2') = y'$. Hence, $\lambda(s, x_1 x_1') = \lambda(s, x_2 x_2') = yy'$, which contradicts the condition that M is a WIFA with delay 1. □

Theorem 4. Let $M = (X, X, S, \delta, \lambda)$ be an n-WIFA with delay 1. If $s \in S$ satisfies $d(s) = \min_{t \in S} d(t)$, then the following items hold .

(1) $d(s)$ is a factor of n, i.e. $n/d(s)$ is an integer.

(2) For any $t \in St(s)$, $d(t) = d(s)$.

(3) For any $y \in Out(s)$, $\mid In(s, y) \mid = n/d(s)$.

(4) If $y \in Out(s)$, then for distinct $s_1, s_2 \in St(s, y)$, $X = \bigcup_{t \in St(s,y)} Out(t)$ and $Out(s_1) \bigcap Out(s_2) = \phi$

(see Fig.5)

Proof. Suppose $Out(s) = \{y_1, y_2, ..., y_d\}$. Then $d(s) = d$. For each $i = 1, 2, ..., d$, denote $In(s, y_i) = \{x_1^i, x_2^i, ..., x_{b_i}^i\}$ and $s_j^i = \delta(s, x_j^i)$ for $j = 1, 2, ..., b_i$. Apparently

$$\sum_{i=1}^{d} b_i = n \qquad \text{(i)}$$

For each i, $Out(s_1^i), Out(s_2^i), ..., Out(s_{b_i}^i)$ are disjoint subsets of X (from Lemma 1.). Hence, we have

$$\sum_{j=1}^{b_i} d(s_j^i) \leq n \qquad \text{(ii)}$$

Acoording to the assumption of s, for any $i = 1, 2, ..., d$ and $j = 1, 2, ..., b_i$,

$$d \leq d(s_j^i) \qquad \text{(iii)}$$

From (ii) and (iii), for $i = 1, 2, ..., d$

$$b_i \cdot d \leq n \qquad \text{(iv)}$$

From (iv) and (i)

$$n = \sum_{i=1}^{d} b_i \leq d \cdot (n/d) = n$$

Hence, the $\leq$ in both (ii) and (iii) should be $=$, i.e.

$d = d(s_j^i)$ and $b_i \cdot d = n$ for $i = 1, 2, ..., d$.

Then we have, $b_1 = b_2 = ... = b_d = n/d$, and we can easily show that (1), (2), (3) and (4) hold true. □

Definition 8. A finite automaton $M = (X, Y, S, \delta, \lambda)$ is said to be strongly connected if $St(s) = S$ for every s in S.

In order to capture the essence of the structure of WIFA, we concentrate on the 'core' of WIFA by removing the 'surplus' states.

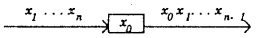

Fig. 6

It is not difficult to see that every finite automaton has a strongly connected subautomaton [12].

If $M = (X, Y, S, \delta, \lambda)$ is a WIFA, then for any s in S, there must exists an integer k such that for any a, a' in X and $\alpha, \alpha' \in x^k, \lambda(s, a\alpha) = \lambda(s, a'\alpha')$ implies $a = a'$. The minimal k satisfying this condition is said to be the delay of s.

Apparently, every state s has a delay $\leq \tau$ and some state s must have delay τ if M is a WIFA with exact delay τ.

Theorem 5. If M is a strongly connected WIFA with exact delay 1, then each state of M has delay 1.

Proof. Let $M = (X, X, S, \delta, \lambda)$, $|X| = n$. At least one $s \in S$ has delay 1, otherwise M is not a WIFA with exact delay 1. Hence $d(s) < n$ (if $d(s) = n$, s has delay 0). From Theorem 4(2), for any $t \in St(s), d(t) = d(s) < n$, i.e. t has delay larger than 0. Since M is a WIFA with exact delay 1, t has delay 1. From the fact that M is strongly connected, $S = St(s)$. □

Theorem 6. If $M = (X, X, S, \delta, \lambda)$ is a strongly connected WIFA with exact delay 1, and if $|X| = p$ is prime, then $d(s) = 1$ for any s in S. Let $x_1x_2...x_p$ be a permutation of X. Then $Out(\delta(s, x_1)), Out(\delta(s, x_2)), ..., Out(\delta(s, x_p))$ is a permutation of X.

Proof. It is immediate from Theorem 4 and Theorem 5. □

Next let's consider a special WIFA with delay 1 over X. Let $M_d = (X, X, X, \delta, \lambda)$, where for $x, y \in X$

$$\delta(x, y) = y$$
$$\lambda(x, y) = x$$

That is, M_d is actually a memory cell over X. For any x_0, x_1, x_2, ..., $x_n \in X$, Fig.6 shows the function of M_d.

We regard M_d as a delay unit. Apparently M_d is a strongly connected WIFA with exact delay 1. We denote $M_d \cdot M_d$ by M_{2d}, similarly the composition of k M_d's by M_{kd}. M_{kd} can be expressed in the form of logical net as shown in Fig.7. M_{kd} is a strongly connected

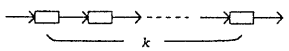

Fig. 7

WIFA with exact delay k.

Theorem 7. If M is a finite automaton over X and M_d a delay unit over X, then $M_dM < MM_d$.

Proof. Let $M = (X, X, S, \delta, \lambda)$. Each state of M_dM is in the form of (x, s), where $x \in X, s \in S$. Similarly, each state of MM_d is in the form of (s, x). For any $s \in S$ and $x, x_1, x_2, ..., x_n \in X$, let $\lambda(s, xx_1x_2...x_n) = y_0y_1y_2...y_n$.

Then $(x, s) \sim (\delta(s, x), \lambda(s, x))$.

Hence, $M_dM < MM_d$. □

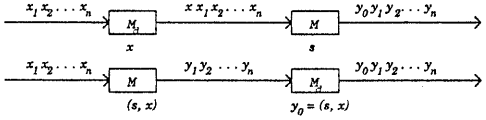

Fig. 8

It is easy to see from Theorem 7 that for any integer k, $M_{kd}M < MM_{kd}$.

Theorem 8. If M is a strongly connected WIFA with exact delay 1 over X and $|X| = p$ is prime, then there exist a WIFA M' with delay 0 such that $M < M'M_d$.

Proof. Let $M = (X, X, S, \delta, \lambda)$. From Theorem 4, for any $s \in S, d(s) = 1$ or p. Since M is a WIFA with exact delay 1, there is s in S such that $d(s) = 1$. Since M is strongly connected, $St(s) = S$. Hence, $d(s) = 1$ for any s in S, i.e. for any x, x' in X, $\lambda(s, x) = \lambda(s, x')$. Define $\lambda(s)$ by $Out(s) = \{\lambda(s)\}$.

Construct $M' = (X, X, S', \delta', \lambda')$, where for $s \in S'$,

$$S' = S$$
$$\delta'(s, x) = \delta(s, x)$$
$$\lambda'(s, x) = \lambda(\delta(s, x))$$

For any s in S', $\lambda'(s, x)$ is a one-one corespondence over X. Hence, M' is a WIFA with delay 0.

From the specifications of δ' and λ', it is not difficult to verify $s \sim (s, \lambda(s))$, where $s \in S$ and $(s, \lambda(s))$ is a state of $M'M_d$. Hence

$$M < M'M_d. \qquad \square$$

Theorem 9. Let $M_1, M_2, ..., M_k$ be strongly connected WIFAs with exact delay 1 over X, and let $|X| = p$ is prime. Then, there exists a WIFA M' with delay 0 over X such that $M_1M_2 \cdots M_k < M'M_{kd}$.

Proof. From Theorem 8, for each $i = 1, 2, ..., k$, there exists a WIFA M_i' with delay 0 suth that $M_i < M_i'M_d$. From Theorem 7, $M_1M_2 \cdots M_k < M_1'M_dM_2'M_d \cdots M_k'M_d < M_1'M_2' \cdots M_k'M_d \cdots M_d = M'M_{kd}$. □

4 Examples of WIFA with Exact Delay 2

Since the decomposition of WIFAs is a new direction in the study of WIFAs, much remains unknown about this subject. We even did not know whether every WIFA can be decomposed into two or more WIFAs with smaller delay. In this section, we prove that there

exist some strongly connected WIFA with exact delay 2 which cannot be decomposed into two WIFAs with delay 1.

Let n be an arbitrary integer greater than one. We consider an n-WIFA over X. Let the elements of X be $x_1, x_2, ..., x_n$. We construct a finite automaton of $2n$ states.

Define $M = (X, X, S, \delta, \lambda)$, where
$S = \{s_i \mid i = 1, 2, ...2n\}$

$\delta(s_i, x_j) = s_{n+j}$ for $i = 1, 2, ..., n$, $j = 1, 2, ..., n$
$\delta(s_{n+i}, x_j) = s_i$ for $i = 1, 2, ..., n$, $j = 1, 2, ..., n$
$\lambda(s_i, x_j) = x_i$ for $i = 1, 2, ..., n$, $j = 1, 2, ..., n$
$\lambda(s_{n+i}, x_j) = x_j$. for $i = 1, 2, ..., n$, $j = 1, 2, ..., n$

Theorem 10. The finite automaton M constructed above has the following properties:

(1) $d(s_i) = 1, d(s_{n+i}) = n$, for $i = 1, 2, ..., n$

(2) for any $x \in X$

$\delta(s_i, x) \in \{s_{n+j} \mid j = 1, 2, ..., n\}$

$\delta(s_{n+i}, x) \in \{s_j \mid j = 1, 2, ..., n\}$

(3) M is a WIFA with exact delay 2, and for $i = 1, 2, ..., n$, s_i has delay 2, s_{n+i} has delay 0.

Proof. (1) and (2) are directly from the definitions of δ and λ.

(3) For any $i = 1, 2, ..., n$, s_{n+i} has delay 0 because $d(s_{n+i}) = n$. Let $u, u' \in X^2$, and $a, a' \in X$. There exist integers $1 \leq f, f', g, g', h, h' \leq n$, such that $a = x_f, a' = x_{f'}, u = x_g x_h, u' = x_{g'} x_{h'}$. then for any $i = 1, 2, ..., n$,

$\lambda(s_i, au) = \lambda(s_i, x_f x_g x_h) = \lambda(s_i, x_f)\lambda(\delta(s_i, x_f), x_g x_h)$
$= x_i \lambda(s_{n+f}, x_g x_h) = x_i x_g \lambda(s_f, x_h) = x_i x_g x_f$

and similarly

$\lambda(s_i, a'u') = \lambda(s_i, x_{f'} x_{g'} x_{h'}) = x_i x_{g'} x_{f'}$.

Then, $\lambda(s_i, au) = \lambda(s_i, a'u')$ implies $x_f = x_{f'}$, i.e. $a = a'$, and s_i has delay 2. It is easy to see from the observation given above that s_i is not of delay 1. Hence M is a WIFA with exact delay 2. □

Next we prove that the M we constructed above cannot be decomposed. First we prove a lemma.

Lemma 2. Let $M = (X, X, S, \delta, \lambda)$ ba a WIFA with delay 1. For any s in S, if $d(s) < |X| = n$, then there exist $x \in X$ such that $d(\delta(s, x)) < n$.

Proof. Let $s \in S$ and $d(s) < |X| = n$. There exist $x_1, x_2 \in X$, $x_1 \neq x_2$, such that $\lambda(s, x_1) = \lambda(s, x_2)$. Since M is a WIFA with delay 1, we must have

$$Out(\delta(s, x_1)) \cap Out(\delta(s, x_2)) = \phi.$$

Hence, both $Out(\delta(s, x_1))$ and $Out(\delta(s, x_2))$ are proper subsets of X, i.e.

$$d(\delta(s, x_1)) < n \text{ and } d(\delta(s, x_2)) < n. \qquad \square$$

Theorem 11. There exists a WIFA with exact delay 2 which cannot be decomposed into two WIFA with delay 1.

Proof. Let us consider the M constructed at the beginning of this section. Suppose $M < M_1 M_2$ for two WIFAs with delay 1 over X. Let $M_1 = (X, X, S_1, \delta_1, \lambda_1)$ and $M_2 = (X, X, S_2, \delta_2, \lambda_2)$.

Denote $M_1 M_2 = (X, X, S_1 \times S_2, \delta_c, \lambda_c)$. Each state of $M_1 M_2$ is of the form (t_1, t_2) for some $t_1 \in S_1$ and some $t_2 \in S_2$. We prove below that for any $s \in S$ and $(t_1, t_2) \in S_1 \times S_2$, it is impossible that $s \sim (t_1, t_2)$.

(1) It is impossible for $s \in \{s_i \mid i = 1, 2, ..., n\}$ to be equivalent to some $(t_1, t_2) \in S_1 \times S_2$. Suppose $s \sim (t_1, t_2)$ for some $s \in \{s_i \mid i = 1, 2, ..., n\}$ and $(t_1, t_2) \in S_1 \times S_2$. Then $d((t_1, t_2)) = d(s) = 1$.

If (a) $d(t_1) < n$, then

from lemma 2, there exists $x \in X$ such that $d(\delta_1(t_1, x)) < n$. Hence,

$d(\delta_c((t_1, t_2), x)) = d(\delta_1(t_1, x), \delta_2(t_2, \lambda_1(t_1, x))) \leq d(\delta_1(t_1, x)) < n$.

However, $d(\delta(s, x)) = d(s') = n$ for some $s' \in \{s_{n+i} \mid i = 1, 2, ..., n\}$. Thus $\delta(s, x)$ is not equivalent to $\delta_c((t_1, t_2), x)$, which contradicts $s \sim (t_1, t_2)$.

If (b) $d(t_1) = n$, then

$d(t_2) = 1$ should hold because $d((t_1, t_2)) = d(t_2)$ in this case. From Theorem 4, $d(\delta_2(t_2, x)) = 1$ for any x in X. Hence, $d(\delta_c((t_1, t_2), x)) \leq d(\delta_2(t_2, \lambda_1(t_1, x))) = 1$ for any x in X. As proved in (a) above, this contradicts $s \sim (t_1, t_2)$.

(2) It is also impossible that $s \sim (t_1, t_2)$ for any $s \in \{s_{n+i} \mid i = 1, 2, ..., n\}$ and $(t_1, t_2) \in S_1 \times S_2$. Otherwise , suppose $s \sim (t_1, t_2)$ for some s in $\{s_{n+i} \mid i = 1, 2, ..., n\}$ and $(t_1, t_2) \in S_1 \times S_2$. Then $\delta(s, x) \sim \delta_c((t_1, t_2), x)$, which contradicts (1) above because $\delta(s, x) \in \{s_i \mid i = 1, 2, ..., n\}$ while $\delta_c((t_1, t_2), x) = (\delta_1(t_1, x), \delta_2(t_2, \lambda_1(t_1, x))) \in S_1 \times S_2$. □

In the proof of Theorem 11, we actually proved a stronger result: each state of the WIFA constructed above cannot be equivalent to any state of the composition of any two WIFAs with delay 1.

5 Binary Case

Due to lack of effecient tools, at present the analysis of non-linear finite automata are very complex and difficult. For the study of the decomposion of WIFAs further, we restrict our WIFAs to binary case in this section, i.e. we only consider the case where the cardinality of the input alphabet is 2.

Let $X = \{x_1, x_2\}$ and $M = (X, X, S, \delta, \lambda)$. Then for any s in S, $d(s) = 1$ or $d(s) = 2$. $d(s) = 2$ means $\lambda(s, x_1) \neq \lambda(s, x_2)$, i.e., s has no delay. If $d(s) = 1$, then $\lambda(s, x_1) = \lambda(s, x_2)$, and in this case we denote it by $\lambda(s)$.

As introduced in Section 1, if M is a WIFA then for any s in S, there exists an integer k such that s has delay k. We denote such k by $delay(s)$. Obviously , M is a WIFA with exact delay τ if and only if $\tau = max_{s \in S}\, delay(s)$.

For any state s and integer k, denote $St(s, k) = \{t \in$

$S \mid t = \delta(s,u)$ for some $u \in X^k\}$.

Theorem 12. Let $M = (X, X, S, \delta, \lambda)$ be a 2-WIFA. Then, $delay(s) = \tau$ $(\tau > 0)$ for every $s \in S$, if and only if that for any $k < \tau$ and $s \in S$

$$| \bigcup_{t \in St(s,k)} Out(t) | = 1 \quad \text{(i)}$$

and

$$\bigcup_{t \in St(\delta(s,x_1),\tau-1)} Out(t) \neq \bigcup_{t \in St(\delta(s,x_2),\tau-1)} Out(t) \quad \text{(ii)}$$

where $X = \{x_1, x_2\}$.

Proof. ($\Longleftarrow$) Suppose for any $s \in S$ and $k < \tau$, (i) and (ii) hold. For k=0, (i) means $d(s) = 1$ for any s in S. Hence (i) implies $\lambda(t) = \lambda(t')$ for any $t, t' \in St(s,k)$, $k < \tau$. Thus for any $u, u' \in X^\tau$, $\lambda(s,u) = \lambda(s,u')$. Hence $delay(s) \neq \tau - 1$. For any $s \in S$ (ii) implies $\lambda(s, x_1 u) \neq \lambda(s, x_2 u')$ for any $u, u' \in X^\tau$ while $\lambda(s, x_1 v) = \lambda(s, x_2 v')$ for any $v, v' \in X^{\tau-1}$. Hence, $delay(s) = \tau$ for any $s \in S$. Therefore, M is a WIFA with delay τ and $delay(s) = \tau$ for any s in S.

($\Longrightarrow$) We prove (i) by induction on k. Suppose that M is a WIFA and $delay(s) = \tau > 0$ for any s in S.

When $k = 0$,

$$\bigcup_{t \in St(s,0)} Out(t) = Out(s).$$

Since delay$(s) = \tau > 0$ implies $d(s) = 1$,

$$| \bigcup_{t \in St(s,0)} Out(t) | = d(s) = 1.$$

Suppose (i) holdes for $k-1 < \tau - 1$. Let us prove that (i) hold for k. We can write

$$\Big(\bigcup_{t \in St(\delta(s,x_1),k-1)} Out(t)\Big) \bigcup \Big(\bigcup_{t \in St(\delta(s,x_2),k-1)} Out(t)\Big) = \bigcup_{t \in St(s,k)} Out(t).$$

From the induction hypothsis,

$$| \bigcup_{t \in St(\delta(s,x_1),k-1)} Out(t) | = | \bigcup_{t \in St(\delta(s,x_2),k-1)} Out(t) | = 1.$$

Next we need to prove

$$\bigcup_{t \in St(\delta(s,x_1),k-1)} Out(t) = \bigcup_{t \in St(\delta(s,x_2),k-1)} Out(t).$$

This is obvious, because otherwise $delay(s) = k < \tau$. Hence

$$| \bigcup_{t \in St(s,k)} Out(t) | = 1$$

for any $s \in S$, $k < \tau$. We must have

$$\bigcup_{t \in St(\delta(s,x_1),\tau-1)} Out(t) \neq \bigcup_{t \in St(\delta(s,x_2),\tau-1)} Out(t),$$

otherwise $| \bigcup_{t \in St(s,\tau)} Out(t) | = 1$, which contradicts $delay(s) = \tau$.

Thus (ii) holds. □

Theorem 13. If M is a 2-WIFA and for any state s of M, $delay(s) = \tau > 0$, then $M < M' M_d$ for some 2-WIFA M', and every state of M' has delay $\tau - 1$.

Proof. Let $M = (X, X, S, \delta, \lambda)$, $X = \{x_1, x_2\}$. For $\tau = 1$ the proof is the same as that of Theorem 8. We next consider the case of $\tau > 1$.

We construct $M' = (X, X, S', \delta', \lambda')$ as follows.

Let

$$S' = S \text{ and for } s \in S',\ x \in X$$
$$\delta'(s,x) = \delta(s,x)$$
$$\lambda'(s,x) = \lambda(\delta(s,x), x).$$

Here, λ' is well-defined because $\delta(s,x) \in S$. Hence $d(\delta(s,x)) = 1$.

For any $s \in S$, $s \sim (s, \lambda(s))$, where $(s, \lambda(s)) \in S' \times X$ is a state of $M' M_d$. This is easy to verify from the definition of δ' and λ'.

Next we prove that M' is a WIFA and delay$(s) = \tau - 1$ for any s in S.

Because M is a WIFA and $delay(s) = \tau$ for any s in S, for any $k < \tau$,

$$| \bigcup_{t \in St(s,k)} Out(t) | = 1$$

and

$$\bigcup_{t \in St(\delta(s,x_1),\tau-1)} Out(t) \neq \bigcup_{t \in St(\delta(s,x_2),\tau-1)} Out(t).$$

By the definition of M', for any $s \in S = S'$

$$\bigcup_{t \in St(s,k)} Out_M(t) = \{x \in X \mid x = \lambda(\delta(s,u), x') \text{ for some } x' \in X \text{ and } u \in X^k\} = \bigcup_{t \in St(s,k+1)} Out_{M'}(t).$$

Here, $Out_M(t)$ and $Out_{M'}(t)$ denote $Out(t)$ with respect to M and M', respectively.

Hence, for any state s of M' and $k < \tau - 1$,

$$| \bigcup_{t \in St(s,k)} Out_{M'}(t) | = 1$$

and

$$\bigcup_{t \in St(\delta(s,x_1),\tau-2)} Out_{M'}(t) \neq \bigcup_{t \in St(\delta(s,x_2),\tau-2)} Out_{M'}(t).$$

From Theorem 12, M' is a WIFA and $delay(s) = \tau - 1$ for any state s of M'. □

Theorem 14. Let M be a 2-WIFA and every state of M has delay τ. Then there exists a 2-WIFA M' with delay 0, such that M can be decomposed into M' and $M_{\tau d}$ (i.e. $M < M' M_{\tau d}$)

Proof. We can prove by repeatedly using Theorm 13

on M. □

Due to the page limit, we omit the proof of the following theorm. However, the major part of the proof is similar to that of Theorem 12, Theorem 13 and Theorem 14.

Theorem 15. Let $M = (X, X, S, \delta, \lambda)$ be a WIFA with exact delay τ. Suppose $k = min_{s \in S}\, delay(s)$, then M can be decomposed into a WIFA with exact delay $\tau - k$ and M_{kd}. □

6 Conclusion

The primary goal of the paper is to explore the decomposability of WIFAs, or more precisely , the decomposability of the delay of WIFAs. The delay of a WIFA is a key factor to the analysis of its structure. Whether a WIFA or what kind of WIFA can be decomposed into WIFAs with smaller delays is, as we have shown in the paper, an important problem. Due to the lack of tools to non-linear case, the only way we can do is to put some restrictions on the WIFAs, and investigate them by combinatorical ways. In this paper, we showed some initial progresses towards the direction. However, much remains to be developed further.

References

[1] F. Bao, *Limited Error-Propagation, Self-Synchronization and Finite Input Memory FSMs as Weak Inverses,* Advances in Chinese Computer Science, Vol.3, World Scientific, Singapore, 1991, 1-24.

[2] F. Bao, Y.Igarashi, *A Randomized Algorithem to Finite Automata Public Key Cryptosystem, ISAAC'94, LNCS,* Springer-Verlag, 1994.

[3] S. Chen, *On the Structure of Finite Automata of which M' Is an (Weak) Inverse Delay τ,* J. of Computer Science and Technology, 1986, Vol.1, No.2, 54-59.

[4] S .Chen, *On the Structure of (Weak) Inverses of an (Weakly) Invertible Finite Automaton,* J. of Computer Science and Technology, 1986, Vol.1, No.3, 92-100.

[5] S. Chen, R. Tao, *The Structure of Weak Inverses of a Finite Automaton with Bounded Error Propagation,* Kexue Tongbao, 1987, Vol.32, No.10, 713-714.

[6] S. Even, *Generalized Automata and Their Information Losslessness,* in Switching Circuit Theory and Logic Design, 1962, 144-147.

[7] S. Even, *On Information Lossless Automata of Finite Order, IEEE* Trans. on Electronic Computers, 1968, Vol.14, No.4, 561-569.

[8] D. A. Huffman, *Canonical Forms for Information-Lossless Finite-State Logic Machines,* IRE Trans. Circuit Theory, 1959, May, 6, Special Supplements, 41-59.

[9] J. L. Massey, M. K. Sain, *Inverse of Linear Seguential Circuits, IEEE* Trans. on Computers, 1968, Vol.17, No.4, 330-337.

[10] J. L. Massey, A. Guber, A. Fisger, *et al., A Self-synchronizing Digital Scrambler for Cryptographic Protection of Data,* in Proceedings of International Zurich Seminar on Digital Communications, March 1984.

[11] R. R. Olson, *A Note on Feedforward Inverses for Linear Sequential Circuits, IEEE* Trans. on Computers, 1970, Vol.19, No.12, 1216-1221.

[12] R. Tao, *Invertibility of Finite Automata,* Academic Press, 1979.(in Chinese)

[13] R. Tao, *On the Relation between Bounded Error Propagation and Feedforwar Inverse,* Kexue Tongbao, 1982, Vol.27, No.7, 406-408.(in Chinese)

[14] R. Tao, *On the Structure of Feedforward Inverse,* Science in China, A., 1983, Vol.26, No.12, 1073-1078.(in Chinese)

[15] R. Tao, S. Chen, *Two Varieties of Finite Automaton Public Key Cryptosystem and Digital Signatures,* J. of Computer Science and Technology, 1986, Vol.1, No.1, 9-18.

[16] R. Tao, *Invertibility of Linear Finite Automata over a Ring, ICALP'88,* Springer-Verlag, 1988, 489-501.

[17] R. Tao, S. Chen, *An Implementation of Identity-Based Crytosystems and Signature Schemes by Finite automaton Public Key Cryptosystems,* in Proceedings of the second National Conference on Cryptography, CRYPTO-CHINA'93, 87-105.(in Chinese)

[18] H. G. Zhang, Z. P. Qin, *et al., The Software Implementation of FA Public Key Cryptosystem,* in Proceedings of the Second National Conference on Cryptography, CRYPTO-CHINA'93, 106-115.(in Chinese)

[19] X. Zhu, *On the Structure of Binary Feedforward Inverses with Delay 2,* J. of Computer Science and Technology, 1989, Vol4. No.2, 163-171.