Finite Automata as Time-Inv Linear Systems Observability, Reachability and More

Radu Grosu

Department of Computer Science, Stony Brook University
Stony Brook, NY 11794-4400, USA

Abstract. We show that regarding finite automata (FA) as discrete, time-invariant linear systems over semimodules, allows to: (1) express FA minimization and FA determinization as particular observability and reachability transformations of FA, respectively; (2) express FA pumping as a property of the FA's reachability matrix; (3) derive canonical forms for FAs. These results are to our knowledge new, and they may support a fresh look into hybrid automata properties, such as minimality. Moreover, they may allow to derive generalized notions of characteristic polynomials and associated eigenvalues, in the context of FA.

1 Introduction

The technological developments of the past two decades have nurtured a fascinating and very productive convergence of automata- and control-theory. An important outcome of this convergence are hybrid automata (HA), a popular modeling formalism for systems that exhibit both continuous and discrete behavior [3,11]. Intuitively, HA are extended finite automata whose discrete states correspond to the various modes of continuous dynamics a system may exhibit, and whose transitions express the switching logic between these modes.

HA have been used to model and analyze embedded systems, including automated highway systems, air traffic management, automotive controllers, robotics and real-time circuits. They have also been used to model and analyze biological systems, such as immune response, bio-molecular networks, gene-regulatory networks, protein-signaling pathways and metabolic processes.

The analysis of HA typically employs a combination of techniques borrowed from two seemingly disjoint domains: finite automata (FA) theory and linear systems (LS) theory. As a consequence, a typical HA course first introduces one of these domains, next the other, and finally their combination. For example, it is not unusual to first discuss FA minimization and later on LS observability reduction, without any formal link between the two techniques.

In this paper we show that FA and LS can be treated in a unified way, as FA can be conveniently represented as discrete, time-invariant LS (DTLS). Consequently, many techniques carry over from DTLS to FA. One has to be careful however, because the DTLS associated to FA are not defined over vector spaces, but over more general semimodules. In semimodules for example, the row rank of a matrix may differ from its column rank.

R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 194–208, 2009.

In particular, we show that: *(1) deterministic-FA minimization and nondeterministic-FA determinization [2] are particular cases of observability and reachability transformations [5] of FA, respectively; (2) FA pumping [2] is a property of the reachability matrix [5] associated to an FA; (3) FA admit a canonical FA in observable or reachable form, related through a standard transformation.*

While the connection between LS and FA is not new, especially from a language-theoretic point of view [2,6,10], our observability and reachability results for FA are to our knowledge new. Moreover, our treatment of FA as DTLS has the potential to lead to a knew understanding of HA minimization, and of other properties common to both FA and LS.

The rest of the paper is organized as follows. Section 2 reviews observability and reachability of DTLS. Section 3 reviews regular languages, FA and grammars, and introduces the representation of FA as DTLS. Section 4 presents our new results on the observability of FA. Section 5 shows that these results can be used to obtain by duality similar results for the reachability of FA. In Section 6 we address pumping and minimality of FA. Finally, Section 7 contains our concluding remarks and directions for future work.

2 Observability and Reachability Reduction of DTLS

Consider a *discrete, time-invariant linear system* (DTLS) with no input, only one output, and with no state and measurement noise. Its $[I, A, C]$, state-space description in left-linear form is then given as below [5]:[1]

$$x(0) = I, \quad x^T(t+1) = x^T(t)A, \quad y(t) = x^T(t)C$$

where x is the *state vector* of dimension n, y is the (scalar) *output*, I is the *initial state vector*, A is the *state transition matrix* of dimension $n\times n$, C is the *output matrix* of dimension $n\times 1$, and x^T is the transposition of x.

Observability. A DTLS is called *observable*, if its *initial state* I can be determined from a sequence of observations $y(0), \ldots, y(t-1)$ [5].

Rewriting the state-space equations in terms of $x(0) = I$ and the given output up to time $t-1$ one obtains the following output equation:

$$[y(0)\ y(1)\ \ldots\ y(t-1)] = I^T\,[C\ AC\ \ldots\ A^{t-1}C] = I^T\,O_t$$

Let X be the *state space* and $W = \text{span}[C\,AC\ldots A^kC\ldots]$ be the *A-cyclic subspace (A-CS) of X generated by C*. Since $C \neq 0$, the dimension of W is $1 \leq k \leq n$, and $[C\,AC\ldots A^{k-1}C]$ is a basis for W [7].[2] As a consequence, for each $t \geq k$, there exist scalars $a_0\ldots a_{k-1}$ such that $A^tC = (C)a_0 + \ldots + (A^{k-1}C)a_{k-1}$.

If $k < n$ then setting $x^T O_t = \sum_{i=0}^{k-1}(A^iC)f_i(x_1,\ldots,x_n)$ to 0 results in k linear equations $f_i(x_1,\ldots,x_n) = 0$ in n unknowns, as A^iC are linearly independent for $i \in [0, k-1]$. Hence, there exist $n-k$ linearly independent vectors x, such that $x^T O_t = 0$, i.e. the dimension of the *null space* $\mathcal{N}(O_t) = \mathcal{N}(O_n)$ is $n-k$ and the *rank* $\rho(O_t) = \rho(O_n) = k$. If $k = n$ then $\mathcal{N}(O_n) = \{0\}$. The set $\mathcal{N}(O_n)$ is called the *unobservable space* of the system because $y(s) = 0$ for all s if $x(0) \in \mathcal{N}(O)$, and the matrix $O = O_n$ is called the *observability matrix*.

[1] The left-linear representation is more convenient in the following sections.

[2] This fact is used by the Cayley-Hamilton theorem.

Basis: $[n_1\ n_2\ \ldots\ n_k]$

Basis: $[q_1\ q_2\ \ldots\ q_k]$

$$\begin{tikzcd} x^T \arrow[r, "A"] & x^T A \arrow[d, "Q"] \\ \overline{x}^T \arrow[u, "Q^{-1}"] \arrow[r, "\overline{A}"] & \overline{x}^T \overline{A} \end{tikzcd}$$

$$\overline{A} = \left[\begin{array}{l} \textbf{ith column: } \text{Representation of} \\ \mathbf{Aq_i} \text{ with respect to } \mathbf{[q_1\ q_2\ \ldots\ q_k]} \end{array}\right]$$

$$Q = [q_1\ q_2\ \ldots\ q_k] \qquad \overline{A} = Q^{-1} A\, Q$$

Fig. 1. Similarity transformations

If $\rho(O) = k < n$ then the *system can be reduced* to an observable system of dimension k. The reduction is done as follows. Pick columns $C, AC, \ldots, A^{k-1}C$ in O and add $n-k$ linearly independent columns, to obtain matrix Q. Then apply the *similarity transformation* $\overline{x}^T = x^T Q$, to obtain the following system:

$$\begin{array}{lllllll} \overline{x}^T(t+1) & = & x^T(t)AQ & = & \overline{x}^T(t)Q^{-1}AQ & = & \overline{x}^T(t)\overline{A} \\ y(t) & = & x^T(t)C & = & \overline{x}^T(t)Q^{-1}C & = & \overline{x}^T(t)\overline{C} \end{array}$$

The transformation is shown in Figure 1, where n_i are the standard basis vectors for n-tuples (n_i is 1 in position i and 0 otherwise), and q_i are the column vectors in Q. Each column i of $\overline{A}$ is the representation of Aq_i in the basis Q, and $\overline{C}$ is the representation of C in Q. Since $q_1, \ldots, q_k$ is a basis for W, all $A_{i,j}$ and C_i for $j \leq k \leq i$ are 0. Hence, the new system has the following form:

$$\begin{array}{rcl} [\overline{x}_o^T(t+1) \quad \overline{x}_{\overline{o}}^T(t+1)] & = & [\overline{x}_o^T(t) \quad \overline{x}_{\overline{o}}^T(t)] \begin{bmatrix} \overline{A}_o & \overline{A}_{12} \\ 0 & \overline{A}_{\overline{o}} \end{bmatrix} \\ y(t) & = & [\overline{x}_o^T(t) \quad \overline{x}_{\overline{o}}^T(t)] \begin{bmatrix} \overline{C}_o \\ 0 \end{bmatrix} \end{array}$$

where $\overline{x}_o$ has dimension k, $\overline{x}_{\overline{o}}$ has dimension $n-k$, and $\overline{A}_o$ has dimension $k \times k$. Instead of working with the unobservable system $[A, C]$ one can therefore work with the *reduced*, observable system $[\overline{A}_o, \overline{C}_o]$ that produces the *same output*.

Reachability. Dually, the system $S = [I, A, C]$ is called *reachable*, if its *final state* C can be uniquely determined from $y(0), \ldots, y(t-1)$. Rewriting the state-space equation in terms of C, one obtains the following equation:

$$[y(0)\ y(1)\ \ldots\ y(t-1)]^T = [I\ (I^T A)^T\ \ldots\ (I^T A^{t-1})^T]^T C = R_t C$$

Since $R_t C = (C^T R_t^T)^T$ and $(I^T A^{t-1})^T = (A^T)^{t-1} I$, the reachability problem of $S = [I, A, T]$ is the observability problem of the *dual* system $S^T = [C^T, A^T, I^T]$. Hence, in order to study the reachability of S, one can study the observability of S^T instead. As for observability, $\rho(R_t) = \rho(R_n)$, where n is the dimension of the state space X. Matrix $R = R_n$ is called the *reachability matrix* of S.

Let $k = \rho(R)$. If $k = n$ then the system is reachable. Otherwise, there is an equivalence transformation $\overline{x}^T = x^T Q$ which transforms S into a reachable system $\overline{S}_r = [\overline{I}_r, \overline{A}_r, \overline{C}_r]$ of dimension k. The reachability transformation of S is the same as the observability transformation of S^T.

3 FA as Left-Linear DTLS

Regular expressions. A *regular expression* (RE) R over a finite set Σ and its associated semantics $L(R)$ are defined inductively as follows [2]: (1) $0 \in \text{RE}$ and

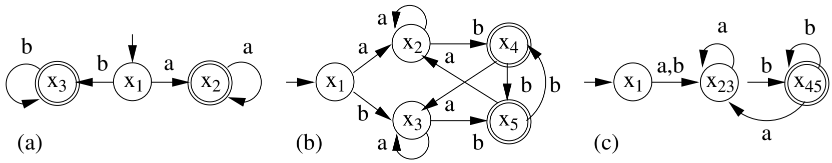

Fig. 2. (a) DFA M_1. (b) DFA M_2. (c) DFA M_3.

$L(0) = \emptyset$; (2) $\epsilon \in \mathrm{RE}$ and $L(\epsilon) = \{\epsilon\}$; (3) If $a \in \Sigma$ then $a \in \mathrm{RE}$ and $L(a) = \{a\}$; (4) If $P, Q \in \mathrm{RE}$ then: $P + Q \in \mathrm{RE}$ and $L(P + Q) = L(P) \cup L(Q)$; $P \cdot Q \in \mathrm{RE}$ and $L(P \cdot Q) = L(P) \times L(Q)$; $P^* \in \mathrm{RE}$ and $L(P^*) = \cup_{n \in \mathbb{N}} L(P)^n$. The denotations of regular expressions are called *regular sets*.[3]

For example, the denotation $L(R_1)$ of the regular expression $R_1 = aa^* + bb^*$, is the set of all strings (or words) consisting of more than one repetition of a or of b, respectively. It is custom to write a^+ for aa^*, so $R_1 = a^+ + b^+$. A *language* L is a subset of Σ^* and consequently any regular set is a (regular) language.

If two regular expressions R_1, R_2 denote the same set one writes $R_1 = R_2$. In general, one can write equations whose indeterminates and coefficients represent regular sets. For example, $X = X\alpha + \beta$. Its *least solution* is $X = \beta\alpha^*$ [2].

The structure $\mathcal{S} = (\Sigma^*, +, \cdot, 0, \epsilon)$ is a *semiring*, as it has the following properties: (1) $\mathcal{A} = (\Sigma^*, +, 0)$ is a commutative monoid; (2) $\mathcal{C} = (\Sigma^*, \cdot, \epsilon)$ is a monoid; (3) Concatenation left (and right) distributes over sum; (4) Left (and right) concatenation with 0 is 0. Matrices $\mathcal{M}_{m \times n}(\mathcal{S})$ over a semiring with the usual matrix sum and multiplication also form a semiring, but note that in a semiring there is *no inverse* operation for addition and multiplication, so the inverse of a square matrix is not defined in a classic sense. If $\mathcal{V} = \mathcal{M}_{m \times 1}(\mathcal{A})$ and *scalar multiplication* is concatenation then $\mathcal{R} = (\mathcal{V}, \mathcal{S}, \cdot)$ is an $\mathcal{S}$-*right semimodule* [10].

Finite automata. A *finite automaton* (FA) $M = (Q, \Sigma, \delta, I, F)$ is a tuple where Q is a finite set of *states*, Σ is a finite set of *input symbols*, $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ is the *transition function* mapping each state and input symbol to a set of states, $I \subseteq Q$ is the set of *initial states* and $F \subseteq Q$ is the set of *final states* [2]. If I and $\delta(q, a)$ are singletons, the FA is called *deterministic* (DFA); otherwise it is called *nondeterministic* (NFA). Three examples of FAs are shown in Figure 2.

Let δ^* extend δ to words. A word $w \in \Sigma^*$ is accepted by FA M if for any $q_0 \in I$, the set $\delta^*(q_0, w) \cap F \neq \emptyset$. The set $L(M)$ of all words accepted by M is called the *language of* M. For example, $L(M_1) = L(a^+ + b^+)$.

Grammars. A *left-linear grammar* (LLG) $G = (N, \Sigma, P, S)$ is a tuple where N is a finite set of *nonterminal symbols*, Σ is a finite set of *terminal symbols* disjoint from N, $P \subseteq N \times (N \cup \Sigma)^*$ is a finite set of *productions*[4] of the form $A \to Bx$ or $A \to x$ with $A, B \in N$ and $x \in \Sigma \cup \{\epsilon\}$, and $S \in N$ is the *start symbol* [2].

A word $a_1 \ldots a_n$ is derived from S if there is a sequence of nonterminals $N_1 \ldots N_n$ in N such that $S \to N_1\, a_1$ and $N_{i-1} \to N_i\, a_i$ for each $i \in [2, n]$. The set $L(G)$ of all words derived from S is called the *language of* G.

[3] The concatenation operator $\cdot$ is usually omitted when writing a regular expression.
[4] It is custom to write pairs $(x, y) \in P$ as $x \to y$.

Equivalence. FAs, LLGs and REs are equivalent, i.e. $L = L(M)$ for some FA M if and only if $L = L(G)$ for some LLG G and if and only if $L = L(E)$ for some RE E [2]. In particular, given an FA $M = (Q, \Sigma, \delta, I, F)$ one can construct an equivalent LLG $G = (Q \cup \{y\}, \Sigma, P, y)$ where P is defined as follows: (1) $y \to q$ for each $q \in F$, (2) $q \to \epsilon$, for $q \in I$, and (3) $r \to q\, a$ if $r = \delta(q, a)$. Replacing each set of rules $A \to \alpha_1, \ldots, A \to \alpha_n$ with one rule $A \to \alpha_1 + \ldots + \alpha_n$ leads to a more concise representation. For example the LLG G_1 derived from M_1 is:

$$x_1 \to \epsilon, \quad y \to x_2 + x_3, \quad x_2 \to x_1\mathtt{a} + x_2\mathtt{a}, \quad x_3 \to x_1\mathtt{b} + x_3\mathtt{b}$$

Each nonterminal denotes the set of words derivable from that nonterminal. One can regard G_1 as a linear system S over REs. One can also *regard* G_1 *as a discrete, time-invariant linear system* (DTLS) S_1 defined as below:

$$x^T(t+1) = x^T(t)A, \quad y(t) = x^T(t)C$$

$$I = \begin{bmatrix} \epsilon \\ 0 \\ 0 \end{bmatrix} \quad A = \begin{bmatrix} 0 & \mathtt{a} & \mathtt{b} \\ 0 & \mathtt{a} & 0 \\ 0 & 0 & \mathtt{b} \end{bmatrix} \quad C = \begin{bmatrix} 0 \\ \epsilon \\ \epsilon \end{bmatrix}$$

The initial state of S_1 is the same as the initial state of DFA M_1 and it corresponds to the production $x_1 \to \epsilon$ of LLG G_1. The output matrix C sums up the words in x_2 and x_3. It corresponds to the final states of DFA M_1 and to the production $y \to x_2 + x_3$ in LLG G_1. Matrix A is obtained from DFA M_1 by taking $v \in A_{ij}$ if $\delta(x_i, v) = x_j$ and $A_{ij} = 0$ if $\delta(x_i, v) \neq x_j$ for all $v \in \Sigma$. The set of all outputs of S_1 over time is $\cup_{t \in \mathbb{N}}\{y(t)\} = I^T A^* C = L(M_1)$.

Matrix A^* can be computed in $\mathcal{R}$ as described in [6]. This provides one method for computing $L(M)$. Alternatively, one can use the least solution of an RE equation, and apply *Gaussian elimination.* This method is equivalent to the *rip-out-and-repair* method for converting an FA to an RE [2].

In the following, all four equivalent representations, RE, FA, LLG and DTLS, of a finite automaton, are simply referred to as an FA. The *observability/reachability* problem for an FA is to determine its initial/final state given $y(t)$ for $t \in [0, n-1]$. In vector spaces, these are unique if the rank of O/R is n. In semimodules however, the *row rank* is generally different from the *column rank.*

4 Observability Transformations of FA

Lack of finite basis. Let I be a set of indices and $\mathcal{R}$ be an $\mathcal{S}$-semimodule. A set of vectors $Q = \{q_i \mid i \in I\}$ in $\mathcal{R}$ is called *linearly independent* if no vector $q_i \in Q$ can be expressed as a linear combination $\sum_{j \in (I-i)} q_j\, a_j$ of the other vectors in Q, for arbitrary scalars $a_j \in \mathcal{S}$. Otherwise, Q is called *linearly dependent.* The independent set Q is called a *basis* for $\mathcal{R}$ if it covers $\mathcal{R}$, i.e. $span(Q) = \mathcal{R}$ [4].

$$E = \begin{array}{c} \begin{array}{ccc} E_0 & E_1 & E_2 \end{array} \\ \begin{bmatrix} 0 & 1\mathtt{a}2{+}1\mathtt{b}3 & 1\mathtt{a}2\mathtt{a}2{+}1\mathtt{b}3\mathtt{b}3 \\ 2 & 2\mathtt{a}2 & 2\mathtt{a}2\mathtt{a}2 \\ 3 & 3\mathtt{b}3 & 3\mathtt{b}3\mathtt{b}3 \end{bmatrix} \end{array} \quad O = \begin{array}{cc} \begin{array}{ccc} C & AC & A^2C \end{array} & \\ \begin{bmatrix} 0 & \mathtt{a}{+}\mathtt{b} & \mathtt{a}^2{+}\mathtt{b}^2 \\ \epsilon & \mathtt{a} & \mathtt{a}^2 \\ \epsilon & \mathtt{b} & \mathtt{b}^2 \end{bmatrix} & \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \end{array}$$

Now consider DFA M_1. Its observability matrix O is given above. Each row i of O consists of the words accepted by M_1 starting in state x_i sorted by their length in increasing order. Each column j of O is the vector $A^{j-1}C$, consisting of the accepted words of length $j-1$ starting in x_i. The corresponding executions E_0, E_1 and E_2 of DFA M_1 are also given above.

The columns of O belong to the *A-cyclic subspace of X generated by C* (A-CS), which has finite dimension in any vector space. In the $\mathcal{S}$-semimodule $\mathcal{R}$, where $\mathcal{S}$ is the semiring of REs, however, A-CS may not have a finite basis.

For example, for DFA M_1 it is not possible to find REs r_{i_j} and vectors $A^{i_j}C$ such that $A^iC = \sum_{j=1}^{k}(A^{i_j}C)r_{i_j}$, for $i_j < i$. Intuitively, abstracting out the states of an FA from its executions, eliminates linear dependencies.

The state information included in E_1 and E_2 allows to capture their linear dependence: E_2 *is obtained from* E_1 *by substituting the last occurrence of states* 2 *and* 3 *with the loops* 2a2 *and* 3a3*, respectively.* Regarding substitution as a multiplication with a scalar, one can therefore write $E_2 = E_1(2\mathtt{a}2 + 3\mathtt{b}3)$.

Indexed boolean matrices. In the above multiplication we tacitly assumed that, e.g. $(1\mathtt{a}2)(3\mathtt{b}3) = 0$, because a b-transition valid in state 3 cannot be taken in states 1 and 2. Treating *independently* the σ-successors/predecessors of an FA $M = (Q, \Sigma, \delta, I, F)$, for each input symbol $\sigma \in \Sigma$, allows to capture this intuition in a "stateless" way. Formally, this is expressed with *indexed boolean matrices* (IBM), defined as follows [12]: (1) $C_i = (i \in F)$; (2) $I_i = (i \in I)$; (2) For each $\sigma \in \Sigma$, $(A_\sigma)_{ij} = (\delta(i,\sigma) = j)$; and (3) $A_{\sigma_1 \ldots \sigma_n} = A_{\sigma_1} \ldots A_{\sigma_n}$. For example, one obtains the following matrices for the DFA M_1:

$$I = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad A_a = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad A_b = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad C = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Indexing enforces a word by word analysis of acceptance and ensures, for example for M_1, that $A_{ab}C = A_a(A_bC) = 0$. Consequently, for every word $w \in \Sigma^*$ the vector A_wC has row i equal to 1, if and only if, w is accepted starting in x_i.

Ordering all vectors $A_{w_i}C$, for $w_i \in \Sigma^i$, in lexicographic order, results in a *boolean observability matrix* $O = [A_{w_0}C \ldots A_{w_m}C]$. This matrix has n rows and $|\Sigma|^n - 1$ columns. Its column rank *is* the dimension of the A-CS W of the *boolean semimodule* $\mathcal{B}$ because all $O_{ij} \in \mathbb{B}$. Hence it is finite and less than $2^n - 1$.

$$O = \begin{array}{c} \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccc} C & A_aC & A_bC & A_{aa}C & A_{ab}C & A_{ba}C & A_{bb}C \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}$$

For example, matrix O for M_1 is shown above. It is easy to see that vectors C, A_aC and A_bC are independent. Moreover, $A_{aa}C = A_aC$, $A_{bb}C = A_bC$. Hence, all vectors A_wC, for $w \in \{a, b\}^*$, are generated by the basis $Q = [C, A_aC, A_bC]$.

The structure of O is intimately related to the states and transitions of the associated FA. Column C is the set of accepting states, and each column A_wC

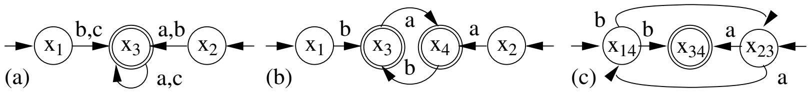

Fig. 3. (a) FA M_4. (b) FA M_5. (c) FA M_6.

is the set of states that can reach C by reading word w. In other words, $A_w C$ is the set of all w-predecessors of C.

In the following we do not distinguish between an FA and its IBM representation. The latter is used to find appropriate bases for similarity transformations and prove important properties about FA. To this end, let us first review and prove three important properties about the ranks of boolean matrices.

Theorem 1. *(Rank independence) If $n \geq 3$ then the* row rank $\rho_r(O)$ *and the* column rank $\rho_c(O)$ *of a boolean matrix O may be different.*

Proof. Consider the observability matrices[5] of FA M_4 and M_5 shown in Figure 3: $\rho_r(O(M_4)) = 3$, $\rho_c(O(M_4)) = 4$, and $\rho_r(O(M_5)) = 4$, $\rho_c(O(M_5)) = 3$.

$$O(M_4) = \begin{array}{c} \begin{array}{cccc} C & A_aC & A_bC & A_cC \end{array} \\ \left[\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right] \end{array} \begin{array}{l} \\ x_1 \\ x_2 \\ x_3 \end{array} \qquad O(M_5) = \begin{array}{c} \begin{array}{ccc} C & A_aC & A_bC \end{array} \\ \left[\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right] \end{array} \begin{array}{l} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}$$

To ensure that an FA is transformed to an equivalent DFA, it is convenient to introduce two more ranks: $\rho_r^d(O)$ and $\rho_c^d(O)$. They represent the number of *distinct* rows and columns in O, respectively. Hence, these ranks consider only linear dependencies in which the sum is identical to its summands.

Theorem 2. *(Rank bounds) The various row and column ranks are bounded and related to each other by the following inequalities:*

$$1 \leq \rho_r(O) \leq \rho_r^d(O) \leq n,\ \ 1 \leq \rho_c(O) \leq \rho_c^d(O) \leq 2^n - 1,\ \ 1 \leq \rho_c(O) \leq C^n_{\lceil n/2 \rceil} + \lfloor n/2 \rfloor$$

Proof. First and second inequalities are obvious. For the third observe that: (1) The set of combinations C_i^n is independent; (2) It covers all C_j^n with $j > i$; (3) Only $i-1$ independent vectors may be added to C_i^n from all C_j^n, with $j < i$.

The A-CS of $\mathcal{B}$ is very similar to the A-CS of a vector space. For example, let $A^k C$ be the set of all vectors $A_w C$ with $|w| = k$. Then the following holds.

Theorem 3. *(Rank computation) If all vectors in $A^k C$ are linearly dependent on a basis Q for $[C\, AC \ldots A^{k-1}C]$, then so are all the ones in $A^j C$, with $j \geq k$.*

Proof. The proof is identical to the one for vector spaces, except that induction is on the length of words in $A_w C$, and $A^k C$ are sets of vectors.

[5] We show only the basis columns of the observability matrix.

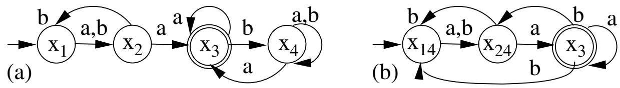

Fig. 4. (a) FA M_7. (b) FA M_8.

Observability transformations. The four ranks discussed above suggest the definition of *four equivalence transformations* $\overline{x}^T = x^T Q$, where Q consists of the independent (or the distinct), rows (or columns) in O, respectively. Each state $q \in Q$ of the resulting FA $\overline{M}$, is therefore a subset of the states of M, and each σ-transition to q in $\overline{M}$ is computed by representing its σ-predecessor $A_\sigma q$ in Q.

Row-basis transformations. These transformations utilize *sets of observably-equivalent states in* M to build the independent states $q \in Q$ of $\overline{M}$. The length of the observations, necessary to characterize the equivalence, is determined by Theorem 3. The equivalence among state-observations itself, depends on whether $\rho_r(O)$ (linear equivalence) or $\rho_r^d(O)$ (identity equivalence) is used.

Using $\rho_r(O)$, one fully exploits linear dependencies to reduce the number of states in $\overline{M}$. For example, suppose that $x_3 = x_1 + x_2$, and that x_1 and x_2 are independent. Then one can replace the states x_1, x_2 and x_3 in M, with states $q_1 = \{x_1, x_3\}$ and $q_2 = \{x_2, x_3\}$ in $\overline{M}$. This generalizes to multiple dependencies, and each new state $q \in Q$ contains *only one* independent state x. Consequently, the language $L(q) = L(x)$. Among the states $q \in Q$, the state C is accepting, and each q that contains an initial state in M is initial in $\overline{M}$.

The transitions among states $q \in Q$ are inferred from the transitions in M. The general rule is that $q_i \xrightarrow{\sigma} q_j$, if all states in q_i are σ-predecessors of the states in q_j. However, as Q is not necessarily a column basis, the σ-predecessor of a state like q_1 above, could be either x_1 or x_3, which are not in Q. Extending x_1 to q_1 does not do any harm, as $L(q_1) = L(x_1)$. Ignoring state x_3 does not do any harm either, as x_3 is covered by x_1 and x_2, possibly on some other path. These completion rules are necessary when computing the "inverse" of Q, i.e. representing AQ in Q to obtain $\overline{A}$.

Theorem 4. *(Row reduction) Given FA M with $\rho_r(O) = k < n$, let R be a* row basis *for O. Define $Q = [q_1, \ldots, q_k]$ as follows: for every $i \in [1, k]$ and $j \in [1, n]$, if row O_j is linearly dependent on R_i then $q_{ij} = 1$; otherwise $q_{ij} = 0$. Then a change of basis $\overline{x}^T = x^T Q$ obeying above completion rules results in FA $\overline{M}$ that: (1) has same output; (2) has states with independent languages.*

Proof. (1) States q satisfy $L(q) = L(x)$, where x is the independent state in q. Transitions $\overline{A}_\sigma = Q^{-1}[A_\sigma q_1 \ldots A_\sigma q_n]$, have $A_\sigma q_i$ as the σ-predecessors of states in q_i. The role of Q^{-1} is to represent $A_\sigma q_i$ in Q. If this fails, it is corrected as discussed above. (2) Dependent rows have been identified with their summands.

For example, consider FA M_7 in Figure 4(a). The observability matrix O of M_7 is given below:[6]

[6] We show only part of the columns in O.

$$O(M_7) = \begin{array}{c} \begin{array}{ccccccc} C & A_aC & A_bC & A_{aa}C & A_{ab}C & A_{ba}C & A_{bb}C \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array} \qquad Q(M_7) = \begin{array}{c} \begin{array}{ccc} q_1 & q_2 & q_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \end{array}$$

Row $x_4 = x_1 + x_2$. This determines the construction of Q as shown above. Using Q in $\overline{x}^T = x^T Q$, results in FA M_8 shown in Figure 4(b). Note that $A_a q_1 = x_4$ has been removed when representing $A_a q_1$ in Q.

Using $\rho_r(O)$ typically results in an NFA, even when starting with a DFA. This is because vectors in Q may have overlapping rows, due to linear dependencies in O. The use of $\rho_r^d(O)$ ensures a resulting DFA, as columns do not overlap.

Identity equivalence also simplifies the transformation. First, Theorem 3 and the computation of ρ_r^d can be performed on-the-fly as a *partition-refinement*: $[C]$, partitions states, based on observations of length 0; $[C\ AC]$, further distinguishes the states in previous partition, based on observations of length 1; and so on. Second, no completion is ever necessary, as Aq is always representable in Q.

Theorem 5. *(Deterministic row reduction) Given an FA M with $\rho_r^d(O) = k < n$ proceed as in Theorem 4 but using $\rho_r^d(O)$. Then if M is a DFA, then so is $\overline{M}$.*

Proof. (1) Theorem 4 ensures correctness. (2) States in Q are disjoint. Hence, no row in $\overline{A} = Q^{-1}AQ$ has two entries for the same input symbol.

For example, let us apply Theorem 5 to the DFA M_2 in Figure 2(b). The corresponding observability matrix is shown below:

$$O(M_2) = \begin{array}{c} \begin{array}{cccc} C & A_bC & A_{ab}C & A_{bb}C \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{array} \qquad Q(M_2) = \begin{array}{c} \begin{array}{ccc} q_1 & q_2 & q_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Rows $x_2 = x_3$ and $x_4 = x_5$. This determines the construction of the basis Q as shown above. Using this basis in the equivalence transformation, results in DFA M_3, which is shown graphically in Figure 2(c).

Corollary 1 (Myhill-Nerode theorem). *Theorem 5 is equivalent to the DFA minimization algorithm of the Myhill-Nerode theorem [2].*

Column-basis transformations. These transformations pick Q as a column basis for O. The definition of basis depends on the notion of linear independence used, and this also impacts the column rank computation via Theorem 3.

Using $\rho_r(O)$, one fully exploits linear dependencies, and chooses a minimal column basis Q as the states of $\overline{M}$. The transitions of $\overline{M}$ are then determined by representing all the predecessors AQ of the states $Q = [q_1 \ldots q_k]$ of $\overline{M}$ in Q. In contrast to the general row transformation, Aq_i, for $i \in [1, k]$, is representable in Q, as Q is a column basis for O. Hence, no completion is ever necessary. Like in vector spaces, the resulting matrices $\overline{A}$ are in *companion form.*

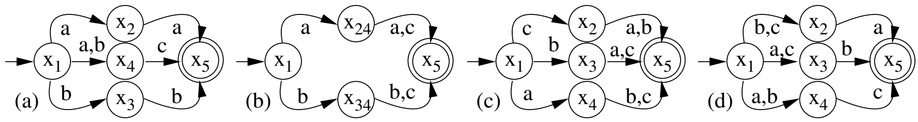

Fig. 5. (a) NFA M_9. (b) DFA M_{10}. (c) DFA M_{11}. (d) NFA M_{12}.

Theorem 6. *(Column reduction) Given an FA M with $\rho_c(O) = k < n$. Define Q as a column basis of O. Then a change of basis $\overline{x}^T = x^T Q$ results in FA $\overline{M}$ with: (1) same output; (2) states with a distinguishing accepting word.*

Proof. (1) Transitions $\overline{A}_\sigma = Q^{-1}[A_\sigma q_1 \ldots A_\sigma q_n]$, have $A_\sigma q_i$ as the σ-predecessors of states in q_i. The role of Q^{-1} is to represent $A_\sigma q_i$ in Q, and this never fails. (2) Dependent columns in O have been identified with their summands.

For example, consider the FA M_5 shown in Figure 3(b) and its associated observability matrix, shown below of Figure 3(b). No row-rank reduction applies, as $\rho_r(O) = 4$. However, as $\rho_c(O) = 3$, one can apply a column-basis reduction, with Q as the first three columns of O. The resulting FA is shown in Figure 3(c).

The column-basis transformation for $\rho_c^d(O)$ simplifies, as dependence reduces to identity. Moreover, in this case $\overline{M}$ can be constructed *on-the-fly*, as follows: Start with $Q, Q_n = [C]$. Then repeatedly remove the first state $q \in Q_n$, and add the transition $p \xrightarrow{\sigma} q$ to $\overline{A}$ for each $p \in Aq$. If $p \notin Q$, then also add p at the end of Q and Q_n. Stop when Q_n is empty. The resulting $\overline{M}^T$ is deterministic.

Theorem 7. *(Deterministic column transformation) Given FA M proceed as in Theorem 6 but using $\rho_c^d(O)$. Then $\overline{M}^T$ is a DFA with $|Q| \leq 2^n - 1$.*

Proof. Each row of $\overline{A}_\sigma^T$ has a single 1 for each input symbol $\sigma \in \Sigma$.

For example, consider the FA M_{11} shown in Figure 5(c). Construct the basis Q by selecting all columns in O. Using this basis in the equivalence transformation $\overline{x}^T = x^T Q$, results in the FA M_{12} shown in Figure 5(d).

5 Reachability Transformations of FA

The boolean semiring $\mathcal{B}$ is *commutative*, that is $ab = ba$ holds. When viewed as a semimodule, left linearity is therefore equivalent to right linearity, that is $\sum_{i \in I} x_i a_i = \sum_{i \in I} a_i x_i$. This in turn means that $(A B)^T = B^T A^T$.

Consequently, in $\mathcal{B}$ the *reachability* of an FA $M = [I, A, C]$ is *reducible* to the *observability* of the FA $M^T = [C^T, A^T, I^T]$, and all the results and transformations in Section 4, can be directly applied without any further proof!

For illustration, consider the FA M_9 shown in Figure 5(a). The reachability matrix $R^T(M_9)$ is given below. It is identical to $O(M_9^T)$.

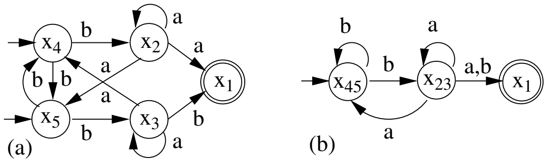

Fig. 6. (a) NFA M_{13}. (b) NFA M_{14}.

$$R^T(M_9) = \begin{array}{c} \begin{array}{ccccccc} I & A_a^T I & A_b^T I & A_{aa}^T I & A_{bb}^T I & A_{ac}^T I & A_{bc}^T I \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{array} \qquad Q(M_9) = \begin{array}{c} \begin{array}{cccc} q_1 & q_2 & q_3 & q_4 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Each row i of R^T corresponds to state x_i. A column $A_w^T I$ of R^T is 1 in row i iff x_i is reachable from I with w^R, or dually, if state x_i accepts w in M^T.[7]

Row-basis transformations. These transformations utilize *sets of reachability-equivalent states in* M to build the independent states $q \in Q$ of $\overline{M}$. These states are, as discussed before, the observability equivalent states of M^T.

Theorem 8. *(Row reduction) Given an FA M, Theorem 4 applied to M^T results in an FA $\overline{M}$ with: (1) same output; (2) states with independent sets of reaching words.*

For example, in $R^T(M_9)$ above, row $x_4 = x_2 + x_3$. This determines the construction of the basis Q, also shown above. Using this basis in the equivalence transformation, results in the DFA M_{10} shown in Figure 5(b).

Identifying linearly dependent states with their generators and repairing lone σ-successors might preclude $\overline{M}^T$ to be a DFA, even if M^T was a DFA. Identifying only states with identical reachability however, ensures it.

Theorem 9. *(Deterministic row reduction) If M^T is a DFA, then Theorem 5 applied to M^T ensures that $\overline{M}^T$ is also a DFA.*

For example, let us apply Theorem 9 to the NFA M_{13} shown in Figure 6(a), the dual of the DFA M_2 shown in Figure 2(b). Hence, $M_{11}^T = M_2$ is a DFA. The reachability matrix $R^T(M_{13})$ is shown below. It is identical to $O(M_2)$.

$$R^T(M_{13}) = \begin{array}{c} \begin{array}{cccc} I & A_b^T I & A_{ab}^T I & A_{bb}^T I \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{array} \qquad Q(M_{13}) = \begin{array}{c} \begin{array}{ccc} q_1 & q_2 & q_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

[7] We write w^R for the reversed form of w.

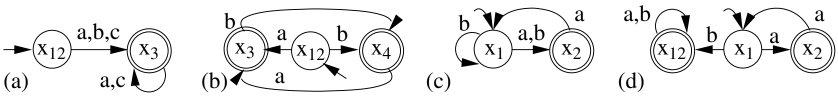

Fig. 7. (a) FA M_{15}. (b) FA M_{16}. (c) FA M_{17}. (d) FA M_{18}.

Rows $x_2 = x_3$ and $x_4 = x_5$. This determines the construction of the basis Q as shown above. Using this basis in the equivalence transformation, results in NFA M_{14}, shown graphically in Figure 6(c). The FA M_{14}^T is a DFA, and $M_{14}^T = M_3$.

Column-basis transformations. Given an FA M, these transformations construct FA $\overline{M}$ by choosing a column basis of R^T as the states Q of $\overline{M}$.

The general form of the transformations uses the full concept of linear dependency, in order to look for a column basis in R^T. Hence, this transformation computes the smallest possible column basis.

Theorem 10. *(Column reduction) Given FA M, Theorem 6 used on M^T results in FA $\overline{M}$ with: (1) same output; (2) states reached with a distinguishing word.*

Consider the NFA M_4 shown in Figure 3(a). Neither a row nor a column-basis observability reduction is applicable to M_4. However, one can apply a column-basis reachability reduction to M_4. The matrix $R^T(M_4)$ is given below.

$$R^T(M_4) = \begin{array}{c} \begin{array}{cccc} I & A_a^T I & A_b^T I & A_c^T I \end{array} \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right] \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \qquad Q(M_4) = \begin{array}{c} \begin{array}{cc} q_1 & q_2 \end{array} \\ \left[\begin{array}{cc} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{array}\right] \end{array}$$

Columns 1 and 2 form a basis for R^T. This determines the construction of Q as shown above. Using Q in $\overline{x}^T = x^T Q$ results in NFA M_{15}, shown in Figure 7(a).

In this case, the column-basis reachability transformation is identical to a row-basis reachability transformation. Consequently, the latter transformation would not require any automatic completion of the σ-successors $q^T A_\sigma$ of $q \in Q$.

Given an FA M, the deterministic column-basis transformation, with column rank $\rho_c^d(R^T)$, always constructs a DFA $\overline{M}$. This construction is dual to the deterministic column-basis observability transformation.

Theorem 11. *(Deterministic column transformation) Given an FA M, Theorem 7 applied to M^T results in the DFA $\overline{M}$.*

Consider for example the NFA M_{17} shown in Figure 7(c). Its reachability matrix $R^T(M_{17})$ is given below, where only the interesting columns are shown.

$$R^T(M_{17}) = \begin{array}{c} \begin{array}{ccc} I & A_a^T I & A_b^T I \end{array} \\ \left[\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right] \end{array} \begin{array}{c} \\ x_1 \\ x_2 \end{array} \qquad Q(M_{17}) = \begin{array}{c} \begin{array}{ccc} q_1 & q_2 & q_3 \end{array} \\ \left[\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right] \end{array}$$

As columns one and two form a basis for R^T, the general column-basis transformation is the identity. The deterministic one is not, as it includes all distinct columns of R^T in Q, as shown above. Using Q in $\overline{x}^T = x^T Q$ results in the DFA M_{18} shown in Figure 7(d). This DFA has one more state, compared to M_{17}.

Applying a deterministic column-basis transformation to an FA M, does not necessarily increase the number of states of M. For example, applying such a transformation to NFA M_6 shown in Figure 3(c), results in the DFA M_{16} shown in Figure 7(b), which has the same number of states as M_6. Moreover, in this case, the general and the deterministic column-basis transformations coincide.

Corollary 2 (NFA determinization algorithm). *Theorem 11 is equivalent to the NFA determinization algorithm [2].*

6 The Pumping Lemma and FA Minimality

In previous sections we have shown that a control-theoretic approach to FA complements, and also allows to extend the reach of, the graph-theoretic approach. In this section we give two additional examples: An alternative proof of the pumping lemma [2]; A alternative approach to FA minimization. Both take advantage of the observability and reachability matrices.

Theorem 12 (Pumping Lemma). *If L is a regular set then there exists a constant p such that every word $w \in L$ of length $|w| \geq p$ can be written as xyz, where: (1) $0 < |y|$, (2) $|xz| \leq p$, and (2) $xy^iz \in L$ for all $i \geq 0$*

Proof. Consider a DFA M accepting L. Since M is deterministic, each column of R^T is a standard basis vector n_i, and there are at most n such distinct columns in R^T. Hence, for every word w of length greater than n, there are words $xyz = w$ satisfying (1) and (2) such that $I^T A_x = I^T A_{xy}$. Since $I^T A_{xy^i} = I^T A_{xy} A_{y^{i-1}}$, it follows that $I^T A_{xy^iz} C = I^T A_w C$, for all $i \geq 0$.

Canonical Forms. Row- and column-basis transformations are related to each other. Let $Q_c \in \mathcal{M}_{i\times j}(\mathcal{B})$, $Q_r \in \mathcal{M}_{i\times k}(\mathcal{B})$ be the observability column and row basis for an FA M. Let $A_c = Q_c^{-1} A Q_c$ and $A_r = Q_r^{-1} A Q_r$.

Theorem 13 (Row and column basis). *There is a matrix $R \in \mathcal{M}_{k\times j}(\mathcal{B})$ such that: (1) $Q_c = Q_r R$; (2) $A_c = R^{-1} A_r R$; (3) $A_r = R A_c R^{-1}$.*

Proof. (1) Let $B(m)$ be the index in O of the independent row of $q_m \in Q_r$ and $C(n)$ be the index in O of the independent column $q_n \in Q_c$, and define $R_{mn} = O_{B(m)C(n)}$, for $m \in [1, k]$, $n \in [1, j]$. Then $Q_c = Q_r R$; (2) As a consequence $A_c = (Q_r R)^{-1} A (Q_r R) = R^{-1} A_r R$; (3) This implies that $A_r = R A_c R^{-1}$.

Hence, A_r is obtained through a reachability transformation with column basis R after an observability transformation with column basis Q_c. Let $\mathcal{O}$ and $\mathcal{R}$ be the column basis observability and reachability transformations, respectively. We call $M_o = \mathcal{O}(\mathcal{R}(M))$ and $M_r = \mathcal{R}(\mathcal{O}(M))$ the *canonical observable* and *reachable* FAs of M, respectively.

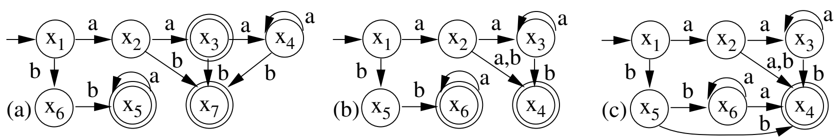

Fig. 8. (a) DFA M_{19}. (b) NFA M_{20}. (c) NFA M_{21}.

Theorem 14 (Canonical FA). *For any FA M, $\mathcal{R}(M_o)=M_r$ and $\mathcal{O}(M_r)=M_o$.*

Minimal FA. Canonical FAs are often *minimal* wrt. to the number of states. For example, M_{11} and M_{12} in Figure 5 are both minimal FAs. Moreover, FA M_{11} is canonical reachable and FA M_{12} is canonical observable.

For certain FAs however, the canonical FAs are not minimal. A *necessary condition* for the lack of minimality, is the existence of a weaker form of linear dependence among the basis vectors of the observability/reachability matrices: A set of vectors $Q = \{q_i \mid i \in I\}$ in $\mathcal{R}$ is called *weakly linearly dependent* if there are two disjoint subsets $I_1, I_2 \subset I$, such that $\sum_{i \in I_1} q_i = \sum_{i \in I_2} q_i$ [8].

For example, the DFA M_{19} in Figure 8(a) has the canonical reachable FA M_{20} shown in Figure 8(b), which is minimal. The observability matrix of M_{20} shown below, has 7 independent columns. The canonical observable FA of M_{19} and M_{20} has therefore 7 states! As a consequence, it is not minimal. Note however, that $A_bC + A_{bb}C = A_{ab}C + A_{ba}C$. Hence, the 7 columns are weakly dependent.

$$O(M_{20}) = \begin{array}{c} \begin{array}{ccccccc} C & A_aC & A_bC & A_{aa}C & A_{ab}C & A_{ba}C & A_{bb}C \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array} \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array} \qquad Q(M_{20}) = \begin{array}{c} \begin{array}{cccccc} q_1 & q_2 & q_3 & q_4 & q_5 & q_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Theorem 15 (Minimal FA). *Given the observability matrix O of an FA M, choose Q as a* set basis *[13] of O, such that AQ is representable in Q. Then the equivalence transformation $\overline{x}^T = x^TQ$ results in a minimal automaton.*

Alternatively, minimization can be reduced to computing the minimal boolean relation corresponding to O. For example, the Karnaugh blocks [9] in $O(M_{20})$ provide several ways of constructing Q. One such way is $Q(M_{20})$ shown above, where one block is the first column in $O(M_{20})$, and the other blocks correspond to its rows. The resulting FA is M_{21}. Both alternatives lead to NP-complete algorithms. Reachability is treated in a dual way, by manipulating R.

Since all equivalent FAs admit an equivalence transformation resulting in the same DFA, and since from this DFA one can obtain all other FAs through an equivalence transformation, *all FAs are related through an equivalence transformation!* This provides a cleaner way of dealing with the minimal FAs, when compared to the *terminal FA (incorporating all other FA)*, discussed in [1].

7 Conclusions

We have shown that regarding finite automata (FA) as discrete, time-invariant linear systems over semimodules, allows to unify DFA minimization, NFA determinization, DFA pumping and NFA minimality as various properties of observability and reachability transformations of FA. Our treatment of observability and reachability may also allow us to generalize the Cayley-Hamilton theorem to FA and derive a characteristic polynomial. In future work, we would therefore like to investigate this polynomial and its associated eigenvalues.

Acknowledgments. I would like to thank Gene Stark and Gheorghe Stefanescu for their insightful comments to the various drafts of this paper. This research was supported in part by NSF Faculty Early Career Award CCR01-33583.

References

1. Nivat, M., Arnold, A., Dicky, A.: A note about minimal nondeterministic automata. EATCS 45, 166–169 (1992)
2. Aho, A.V., Ullman, J.D.: The Theory of Parsing, Translation and Compiling. Prentice-Hall, Englewood Cliffs (1972)
3. Alur, R., Coucoubetis, C., Halbwachs, N., Henzinger, T.A., Ho, P.H., Nicolin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. Theoretical Computer Sciences 138, 3–34 (1995)
4. Beasley, L.B., Guterman, A.E., Jun, Y.B., Song, S.Z.: Linear preservers of extremes of rank inequalities over semirings: Row and column ranks. Linear Algebra and its Applications 413, 495–509 (2006)
5. Chen, C.T.: Linear System Theory Design. Holt, Reinhart and Winston (1984)
6. Conway, J.H.: Regular Algebra and Finite Machines. Chapman and Hall, Boca Raton (1971)
7. Friedberg, S.H., Insel, A.J., Spence, L.E.: Linear Algebra. Prentice-Hall, Englewood Cliffs (1989)
8. Gondran, M., Minoux, M.: Graphs, Dioids and Semirings: New Models and Algorithms. Springer, Heidelberg (2008)
9. Karnaugh, M.: The map method for synthesis of combinational logic circuits. Transactions of American Institute of Electrical Engineers 72(9), 593–599 (1953)
10. Kuich, W., Salomaa, A.: Semirings, Automata, Languages. Springer, Heidelberg (1986)
11. Lynch, N., Segala, R., Vaandrager, F.: Hybrid I/O automata. Information and Computation 185(1), 103–157 (2003)
12. Salomaa, A.: Theory of Automata. Pergamon Press, Oxford (1969)
13. Stockmeyer, L.J.: The set basis problem is NP-complete. Technical Report RC-5431, IBM (1975)