ON 2PFA's AND THE HADAMARD QUOTIENT OF FORMAL POWER SERIES *

Marcella Anselmo   Alberto Bertoni

Abstract

We present the main results on 2PFA's and on the Hadamard quotient of formal power series, the connection between the two notions being a result stating that the event defined by a 2PFA is the Hadamard quotient of two rational power series.

1 Introduction

A two-way probabilistic finite automaton (2PFA) is a machine consisting of a probabilistic finite-state control and an input tape which is scanned by a single two-way head, that is, the head can move both left and right.

The Hadamard quotient of rational power series φ and ψ is the power series associating with a string x the quotient $\varphi(x)/\psi(x)$, whenever defined.

With every 2PFA, it can be associated a power series called the *event*, that is the series associating to a string its probability to be accepted by the 2PFA. In the opposite to the one-way case, the event defined by a 2PFA is not always a rational power series. What turns out, and it is the motivation of this double subject paper, is that events defined by 2PFA's can be expressed in terms of rational power series; namely they are always the Hadamard quotient of two rational power series.

In Section 2 we present some classical results on the computational power of probabilistic automata pointing out the relationships between the two-way case and the one-way case.

Section 3 concerns the literature on the Hadamard quotient of power series. The most of the works on this subject deal with power series on one-letter alphabets and consider some analytical problems such as some partial solutions to the Pisot's conjecture, the conjecture asking whether the Hadamard quotient of two rational power series is still rational. On the contrary, in [1, 2] it is investigated the class $\mathcal{H}ad(K, \Sigma)$ which is the closure of rational power series by the Hadamard inverse, in the general case of a several letters alphabet.

Section 4 states the relation between 2PFA's and the Hadamard quotient, i.e. the result stating that the event defined by a 2PFA is always the Hadamard quotient of

*This work was partially supported by ESPRIT-EBRA project ASMICS contract 6317 and project 40% MURST "Algoritmi, Modelli di Calcolo e Strutture Informative".

Received by the editors April 1993, revised December 1993.
Communicated by M. Boffa.
AMS Mathematics Subject Classification : 68Q68, 68Q45.
Keywords : two-way probabilistic automata, events, formal power series, Hadamard quotient.

two rational power series. It then shows some consequences arising from this result, among which new proofs to some already known results. In particular, we present some decidability results and the inclusions among the classes of languages defined from 2PFA's and 1PFA's. Most of results in Section 4 can be found in [1, 2].

2 Probabilistic Automata

The research on probabilistic machines was initiated in 1956 by a fundamental paper by de Leeuw, Moore, Shannon and Shapiro [7].

Rabin [22] considered (one-way) probabilistic automata (1PFA), introduced the notion of recognition of a language by a 1PFA with cut-point and understood the importance of isolation of the cut-point. References to probabilistic automata are [20, 24].

A *one-way probabilistic finite automaton* (1PFA) $\mathcal{A}$ over an alphabet Σ is a 4-tuple $\mathcal{A} =< Q, \pi, \{A(\sigma)/\sigma \in \Sigma\}, \eta >$, where $Q = \{q_1, q_2, \ldots, q_m\}$ is a finite set of states; π is a $1 \times m$ stochastic vector representing the initial probabilities; $\forall \sigma \in \Sigma$, $A(\sigma)$ represents the transition probabilities and it is a $m \times m$ stochastic matrix ; η is a $m \times 1$ vector with 0 and 1 entries, interpretable as the characteristic vector of the final states. We recall that a matrix is said stochastic if it has entries in the interval $[0, 1]$ with each row sum equals to 1.

The *event* defined by $\mathcal{A}$ is $P_{\mathcal{A}} : \Sigma^* \to [0, 1]$ where $P_{\mathcal{A}}(a_1 a_2 \cdots a_k) = \pi A(a_1) A(a_2) \cdots A(a_k)\eta$ is the accepting probability of a word $w = a_1 a_2 \cdots a_k \in \Sigma^*$. We observe that Kleene-Schützenberger's Theorem stating that a power series is rational iff it is recognized by a one-way automaton with multiplicity in a semiring [11], guarantees that the event defined by a 1PFA is always a rational power series. In fact a 1PFA can be regarded to as a one-way automaton with multiplicity. The *language accepted* by a 1PFA $\mathcal{A}$ with *cut-point* $\lambda \in [0, 1]$ is $T(\mathcal{A}, \lambda) = \{w \in \Sigma^*/P_{\mathcal{A}}(w) > \lambda\}$. The cut-point λ is *isolated* w.r.t. $\mathcal{A}$ if there exists $\varepsilon > 0$ such that $|P_{\mathcal{A}}(w) - \lambda| \geq \varepsilon, \forall w \in \Sigma^*$. A language accepted by a 1PFA with cut-point is said *stochastic*.

In his fundamental paper of 1963 [22], Rabin showed that 1PFA's, on the contrary to their deterministic counterpart, can also accept nonregular languages. He provided the example of a 1PFA accepting a word $w = a_1 a_2 \cdots a_k \in \{0, 1\}^*$ with probability equals to the 10-base representation of the number $0.a_1 a_2 \cdots a_k$. This means that the sets $T(\mathcal{A}, \lambda)$ for $0 \leq \lambda < 1$ form a nondenumerable family of languages, while the regular languages are a denumerable family.

The situation is different if the cut-point is requested to be isolated. Rabin proved that 1PFA's with isolated cut-point recognize only regular languages. In other terms regular languages are the only languages that can be effectively recognized by 1PFA's using statistical methods for estimating the accepting probability of a word.

It is important to observe that, as shown by Gill, a probabilistic automaton that accepts a language with ε-isolated cut-point λ corresponds to a probabilistic automaton that computes with $(\lambda - \varepsilon)$ bounded error probability [14].

Another important result on 1PFA's is Turakainen's Theorem [25, 24], stating that the language $\{w/(\eta, w) > 0\}$ for all rational power series η is stochastic. In other terms it proves that 1PFA's recognize exactly the positive parts of R-rational series, showing therefore that stochastic languages can be defined in a purely non probabilistic way.

The definition of 2PFA's was introduced in 1973 by Kuklin in [17], that did not consider language recognition. A two-way probabilistic finite automaton consists of a probabilistic finite-state control and an input tape which is scanned by a single two-way head, that is, the head can move both left and right.

Different formal definitions are possible, following that we put the endmarkers at the ends of the word on the input tape or not, or we allow an accepting computation ending on any position of the word or only on the right endmarker, and so on.

We will consider the following definition. A *two-way probabilistic finite automaton* (2PFA) $\mathcal{A}$ over an alphabet Σ is a 4-tuple $\mathcal{A} =< Q, \pi, \{A(\sigma, L), A(\sigma, R)/\sigma \in \Sigma\}, \eta >$, where $Q = \{q_1, q_2, \ldots, q_m\}$ is a finite set of states; π is a $1 \times m$ stochastic vector representing the initial probabilities; $A(\sigma, L)$ and $A(\sigma, R)$ represent the transition probabilities to the left and to the right respectively, and are $m \times m$ matrices with nonnegative real entries such that $A(\sigma, L) + A(\sigma, R)$ is stochastic $\forall \sigma \in \Sigma$; η is a $m \times 1$ vector with 0 and 1 entries, interpretable as characteristic vector of the final states. A *computation* on input w begins with the head scanning the leftmost symbol of w in state q_i with probability π_i and runs according to the transition probabilities given by matrices $A(\_, \_)$. In a computation it is forbidden to move off the left end of the input. The *event* defined by $\mathcal{A}$ is $P_{\mathcal{A}} : \Sigma^* \rightarrow [0, 1]$ where $P_{\mathcal{A}}(w)$ is the probability that the automaton in a computation on $w \in \Sigma^*$ moves off the right end entering a final state.

The first results on probabilistic 2-way machines were presented by Freivalds [12]. In the oppposite to Rabin's result, Freivalds showed that 2PFA's can recognize nonregular languages also when the cut-point is restricted to be isolated. The language $\{0^n 1^n / n \in N\}$ is an example.

Dwork and Stockmeyer [10] completed this result showing that if a 2PFA recognizes a nonregular language with isolated cut-point, then it requires time 2^{n^b} infinitely often, for a positive constant b. Moreover, this time bound cannot be improved as shown by Kaneps and Freivalds [16].

Dwork and Stockmeyer also considered the utilization of 2PFA's in cryptography [8, 9, 10]. They investigated interactive proof systems and zero-knowledge interactive proof systems where the verifier is a 2PFA.

3 The Hadamard quotient

Given a finite alphabet Σ, let $< \Sigma^*, ., \varepsilon >$ be the free monoid generated by it. Given a semiring K, the class $K \ll \Sigma \gg$ of *formal power series* in non-commuting variables in Σ and coefficients in K is the set of functions $s : \Sigma^* \rightarrow K$. As usual, the value of s on $w \in \Sigma^*$ is denoted by (s, w) and referred to as the *coefficient* of the series. The power series is written as a formal sum $s = \sum_{w \in \Sigma^*} (s, w) w$. The family of K*-rational* power series on Σ is the smallest family containing the polynomials and closed with respect to sum, Cauchy product and *.

References to formal power series are [5, 18, 24]. The *Hadamard product* of s, $t \in\leftarrow K \ll \Sigma \gg$ is defined as $s \otimes t = \sum_{w \in \Sigma^*} (s, w)(t, w) w$. It is well-known that the family of K*-rational* power series is closed under Hadamard product when K is a commutative semiring. The identity element for $\otimes$ is the power series $1 = \sum_{w \in \Sigma^*} w$. The *Hadamard quotient* s/t of s by t is the Hadamard product of s by the Hadamard inverse of t, whenever it exists. In fact, the Hadamard inverse of s exists iff $(s, w) \neq 0$ for all $w \in \Sigma^*$; in this case it is the series $1/s = \sum_{w \in \Sigma^*} 1/(s, w)w$.

Let $Rat(\Sigma, K)$ be the class of K-rational power series with respect to $+$, $\otimes$. Remark that the class $Rat(\Sigma, K)$ is not closed under the Hadamard inverse. For example, the Hadamard inverse of $s = 1 + \sigma^*\sigma\sigma^* = 1 + \Sigma n\sigma^n$ exists but it is not in $Rat(\Sigma, K)$. The class $\mathcal{H}ad(K, \Sigma)$ is the closure of rational power series by the Hadamard inverse, in the general case of a several letters alphabet Σ.

The Hadamard product of two rational power series is still a rational power series when K is a commutative semiring. The situation is more complicated when the Hadamard quotient is considered. The problem of stating whether the Hadamard quotient of two rational power series is rational has been solved only in a particular case, when a one-letter alphabet is considered. The Pisot's conjecture has been shown true in [21, 26] (see also [23]) after many years of researches. It can be stated as follows.

Theorem 3.1 *(Pisot's Conjecture) Let $\Sigma s_n z^n$ and $\Sigma t_n z^n$ two rational power series with coefficients in a 0-characteristic field K. If every t_n is different from 0 and there exists a subsemiring A of K such that $s_n/t_n \in A$ for all n, then the power series $\Sigma s_n/t_n z^n$ is rational.*

The Hadamard algebra of power series on a one-letter alphabet has been extensively studied by B. Benzaghou in his thesis [3]. He studied some of its sub-algebras. In particular, the Hadamard algebra obtained from rational power series and its rationality preserving operations. This thesis also contains an attempt to the solution of the Pisot's Conjecture, not yet proved at that time, i.e. some sufficient conditions for it holds, these being of a strictly arithmetic nature.

Other works related with the Hadamard quotient of power series are [4, 6, 13, 19]. The most of these works deal with power series on one-letter alphabets and consider some analytical problems such as some partial solutions to the Pisot's conjecture or its possible extensions.

In [1, 2] problems of a different kind are considered. The class $\mathcal{H}ad(K, \Sigma)$ on a generic finite alphabet Σ is investigated and characterized as follows : $\mathcal{H}ad(K, \Sigma) = \{\varphi/\psi$ such that $\varphi, \psi \in Rat(K, \Sigma)$ and $\psi(w) \neq 0\ \forall w \in \Sigma^*\}$. Some decidability results on $\mathcal{H}ad(K, \Sigma)$ are shown. In [2] the interest is devoted to power series with coefficients in $Q \ll z \gg$. It is considered the derivative series of a series in $\mathcal{H}ad(Q \ll z \gg, \Sigma)$ and shown that it is still in $\mathcal{H}ad(Q \ll z \gg, \Sigma)$. The other main results of [1, 2] are the subject of next Section.

4 2PFA's and the Hadamard quotient

The results of this Section are contained in [1, 2].

Kleene-Schützenberger's Theorem does not extend to the two-way case, that is power series recognized by two-way automata with multiplicity are not always rational power series. Moreover, events defined by 2PFA's are not always rational power series. For example, consider the one state 2PFA on the alphabet $\Sigma = \{a\}$

which moves with equal probability to the right and to the left. The event defined by it associates with the word a^k the quantity $1/(k+1)$, realizing a nonrational power series [1].

In order to present some results on the nature of events defined by 2PFA's let us give some definitions. Given $w \in \Sigma^*$ and $1 \leq t \leq| w |$, state q is said (t, w)-*absorbing* if the automaton beginning in state q scanning the t-th letter of w does not admit any computation moving off some end with a non zero probability but there are an infinite number of computations reentering state q on the t-th symbol of w. If no state is absorbing, the automaton is said *transient*. Let $p_n(w)$ be the probability that w is accepted by $\mathcal{A}$ in n steps.

Let us now consider the class $\mathcal{H}ad(Q \ll z \gg, \Sigma)$ of power series with coefficients in $Q \ll z \gg$. Let $s \in \mathcal{H}ad(Q \ll z \gg, \Sigma)$. The *derivative* of s is $s' = \sum_{w\in\Sigma^*} d/dz(s, w)w$.

Theorem 4.1 *([2]) Given a 2PFA $\mathcal{A}$ on Σ the power series*

$$f_{\mathcal{A}} = \sum_{w\in\Sigma^*} \sum_{n\in N} p_n(w)z^n w$$

belongs to $\mathcal{H}ad(Q \ll z \gg, \Sigma)$.

This result allows us to show that the event defined by a 2PFA, the average time of a 2PFA and its variance are power series in $\mathcal{H}ad(Q, \Sigma)$. The average time to compute w is defined as $AVT(w) = \sum_{n\in N} np_n(w)$ and its variance as $VAR(w) = \sum_{n\in N} n^2 p_n(w) - (\sum_{n\in N} np_n(w))^2$.

Corollary 4.2 *The event defined by a transient 2PFA, the average time and its variance are all in $\mathcal{H}ad(Q, \Sigma)$.*

Proof. (outline) Let $h_1 : Q \ll z \gg \rightarrow Q$ be the evaluation in 1, that is the homomorphism mapping z to 1. If $s \in \mathcal{H}ad(Q \ll z \gg, \Sigma)$ then $h_1 s \in \mathcal{H}ad(Q, \Sigma)$, because h_1 is a semiring homomorphism. The goal now follows from the fact that the derivative of a series in $\mathcal{H}ad(Q \ll z \gg, \Sigma)$ is still in $\mathcal{H}ad(Q \ll z \gg, \Sigma)$ [2] and from :

(i) $P_{\mathcal{A}} = h_1 \cdot f_{\mathcal{A}}$;
(ii) $AVT = h_1 \cdot (f_{\mathcal{A}})'$;
(iii) $VAR = h_1 \cdot (f_{\mathcal{A}})' + h_1 \cdot (f_{\mathcal{A}})'' - (h_1 \cdot f'_{\mathcal{A}})^2$.

Note that only with transient 2PFA's we are sure that the evaluation h_1 of $f_{\mathcal{A}}$ and its derivatives are defined, that is they are not a quotient with a 0 denominator. ■

Remark that Corollary 4.2 extends to the case of nontransient 2PFA's, but this case needs a more complex proof. The proof that events defined by transient and nontransient 2PFA's are in $\mathcal{H}ad(Q, \Sigma)$ is shown in [1].

Some words about the proof of Theorem 4.1 (for an outline see [2]). The proof extends the one given in [1] to show that events defined by 2PFA's are in $\mathcal{H}ad(Q, \Sigma)$. It involves introducing some Markov chains and computing the closure of matrices with entries in $Q \ll z \gg$. Furthermore, the proof is constructive.

The construction is exponential in the case of transient automata, but becomes more complicated in the case of nontransient automata. This reflects a difficulty also encountered by Kaneps when dealing with nontransient 2PFA's in [15]. In order to show the stochasticity of languages recognized by 2PFA's, he provides a construction, also based on Markov chains, that becomes more than exponential in the case of nontransient 2PFA's. He states as an open problem the possibility of reducing the complexity of this problem.

Corollary 4.2 says in particular that the class of events defined by 2PFA's is included in the class of Hadamard quotient of rational power series. The inclusion is strict. This can be shown considering the language *Pali* of palindrome words on the alphabet $\Sigma = \{0, 1\}$. In fact, it can be rather easily constructed a power series η in $\mathcal{H}ad(Q, \Sigma)$ such that $Pali = \{w/(\eta, w) > \lambda\}$ with an isolated λ. On the other hand, Dwork and Stockmeyer proved that there exists no 2PFA that can recognize *Pali* with an isolated cut-point [8].

4.1 Some decidability results

Some decidability results on $\mathcal{H}ad(K, \Sigma)$[1] immediately follow from classical decidability results on $Rat(K, \Sigma)$, (see [5, 18, 24]). In particular we have the following

Corollary 4.3
(i) It is undecidable whether or not a series in $\mathcal{H}ad(K, \Sigma)$ admits its Hadamard inverse;
(ii) it is decidable whether or not two series in $\mathcal{H}ad(K, \Sigma)$ are equivalent (i.e. have same coefficients);
(iii) the coefficients of a given series in $\mathcal{H}ad(K, \Sigma)$ are computable.

Theorem 4.1 has the following results as a corollary.

Corollary 4.4 *It is decidable whether two 2PFA's define the same event and whether a string is accepted by a given 2PFA with probability greater than a given value.*

The problem of the membership of a word to the language accepted by a 2PFA was already proved decidable by Freivalds [12]. In [1] it is also proved that the problem is in NC^2.

4.2 Classes of languages

Let state the following notation :
$\mathcal{L}(1PFA)$ is the set of languages recognized by 1PFA's with cut-point;
$\mathcal{L}_{is}(1PFA)$ is the set of languages recognized by 1PFA's with isolated cut-point;
$\mathcal{L}(2PFA)$ is the set of languages recognized by 2PFA's with cut-point;
$\mathcal{L}_{is}(2PFA)$ is the set of languages recognized by 2PFA's with isolated cut-point.

Proposition 4.5

$$\mathcal{L}(1PFA) = \mathcal{L}(2PFA) \supset \mathcal{L}_{is}(2PFA) \supset \mathcal{L}_{is}(1PFA) = Reg$$

where $\supset$ denotes the proper inclusion and Reg is the set of all regular languages.

Proof. (outline)

(i) $\mathcal{L}(1PFA) = \mathcal{L}(2PFA)$

By Theorem 4.1, for all 2PFA $\mathcal{A}$ we have $T(\mathcal{A}, \lambda) = \{w : (r, w) > 0\}$ where r is the rational power series $r = (\varphi - \lambda\psi) \otimes \psi$. Turakainen's Theorem [25, 24], as recalled in Section 2, completes the proof. Another different proof is given by Kaneps in [15].

(ii) $\mathcal{L}(2PFA) \supset \mathcal{L}_{is}(2PFA)$

The proper inclusion is shown considering the language of palindrome words on the alphabet $\Sigma = \{0, 1\}$. This language belongs to $\mathcal{L}(2PFA)$ because there exists a rational power series η such that $Pali = \{w/(\eta, w) > 0\}$. That implies that the language is stochastic by the above mentioned Turakainen's Theorem. On the contrary, Dwork and Stockmeyer in [8] showed that it cannot be recognized by a 2PFA with isolated cut-point.

(iii) $\mathcal{L}_{is}(2PFA) \supset \mathcal{L}_{is}(1PFA)$

Freivalds in 1981 showed that 2PFA's with isolated cut-point can also recognize nonregular languages and this shows the goal in view of point (iv).

(iv) $\mathcal{L}_{is}(1PFA) = Reg$ [22].

∎

References

[1] M. Anselmo and A. Bertoni, Two-way Probabilistic Automata and Rational Power series, *Proc. IV Conv. It. Inform. Teor.*, L'Aquila October 28/30 1992, World Scientific, 9–23.

[2] M. Anselmo and A. Bertoni, On the Hadamard quotient of Rational Power series : an application, Poster at *V Formal Power Series and Algebraic Combinatorics*, Firenze June 21/25 1993.

[3] B. Benzaghou, Algèbres de Hadamard, *Bull. Soc. Math. France* **98** (1970) 209–252.

[4] J. Berstel, Sur les pôles et le quotient de Hadamard de séries N-rationnelles, *C.R. Acad. Sc. Paris* **272**, série A (1971) 1079–1081.

[5] J. Berstel and C. Reutenauer, *Rational Series and their languages*, Springer Verlag, New York (1988).

[6] J.P. Bézivin, Quotient de fonctions entières et quotients de Hadamard de séries formelles, *Ann. Inst. Fourier*, Grenoble **39** (3) (1989) 737–752.

[7] K. de Leeuw, E.F. Moore, C.E. Shannon and N. Shapiro, Computability by probabilistic machines, in Automata Studies, *Ann. Math. Studies* **34**, Princeton Univ. Press (1965) 183–212.

[8] C. Dwork and L. Stockmeyer, Zero-Knowledge With Finite State Verifiers, *Proc. CRYPTO 1988*, LNCS **403** (1988) 71–75.

[9] C. Dwork and L. Stockmeyer, On the power of 2-way Probabilistic Finite State Automata, *Proc. FOCS 89* (1989) 480–485.

[10] C. Dwork and L. Stockmeyer, A time complexity gap for two-way probabilistic finite-state automata, *SIAM J. of Comput.* **19** (6) (1990) 1011–1023.

[11] S. Eilenberg, *Automata, Languages and Machines* vol. A, Academic Press (1974).

[12] R. Freivalds, Probabilistic Two-way Machines, in *Proc. Int. Symp. on Math. Found. of Comp. Sc.*, LNCS **118** (1981) 333–345.

[13] K. Gérardin, Quotient de Hadamard de series rationnelles en variables non commutatives, *Proc. Ecole de Printemps d'Inform. Théor.* may 23/27 1977, 119–134.

[14] J. Gill, Computational commplexity of probabilistic Turing machines, *SIAM J. Comput.* **6** (1977) 675–695.

[15] J. Kaneps, Stochasticity of the languages acceptable by two-way finite probabilistic automata, *Diskretnaya matematika* **4** (1989) (Russian).

[16] J. Kaneps and R. Freivalds, Running time to recognize nonregular languages by two-way probabilistic automata, *Proc. ICALP 91, LNCS* **510** (1991) 174–185.

[17] Yu. I. Kuklin, Two-way Probabilistic Automata, *Avtomatika i vycislitelnaja tekhnika* **5** (1973) 35–36 (Russian).

[18] W. Kuich and A. Salomaa, *Semirings, Automata, Languages*, EATCS Monographs on Theor. Comp. Sc. 5, Springer Verlag, Berlin (1986).

[19] G. Pathiaux, Algèbres de Hadamard de fractions rationnelles, *C.R. Acad. Sc. Paris*, **267**, série A (1968) 977–979.

[20] A. Paz, *Introduction to Probabilistic Automata*, Academic Press (1971).

[21] Y. Pourchet, Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles, *C.R. Acad. Sc. Paris* **288**, série A (1979) 1055–1057.

[22] M.O. Rabin, Probabilistic Automata, *Inform. and Control* **6** (1963) 230–245; and in *Sequential machines*, E.F. Moore ed., Addison Wesley (1964).

[23] R. Rumely, Notes on Van der Poorten's proof of the Hadamard quotient theorem, *Séminaire de Th. de Nombres de Paris.*

[24] A. Salomaa and M. Soittola, *Automata-theoretic aspects of formal power series*, Springer (1978).

[25] P. Turakainen, Generalized automata and stochastic languages, *Proc. Amer. Math. Soc.* **21** (1969) 303–309.

[26] A.J. Van der Poorten, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, *C.R. Acad. Sc. Paris* **306**, série I (1988) 97–102.

Marcella Anselmo
Dip. di Informatica ed Appl.
Università di Salerno
I-84081 Baronissi (SA)
Italia
tel. (39) +89 822405
e-mail : anselmo@udsab.dia.unisa.it

Alberto Bertoni
Dip. di Informatica ed Appl.
Università di Milano
Via Comelico, 39
I-20135 Milano
Italia