The Product of Rational Languages

Imre Simon*

Instituto de Matemática e Estatística
Universidade de São Paulo
05508-900 São Paulo, SP, Brasil
<is@ime.usp.br>

Abstract. The very basic operation of the product of rational languages is the source of some of the most fertilizing problems in the Theory of Finite Automata. Indeed, attempts to solve McNaughton's star-free problem, Eggan's star-height problem and Brzozowski's dot-depth problem, all three related to the product, already led to many deep and ever expanding connections between the Theory of Finite Automata and other parts of Mathematics, such as Combinatorics, Algebra, Topology, Logic and even Universal Algebra. We review some of the most significant results of the area, obtained during the last 35 years, and try to show their contribution to our understanding of the product.

1 Introduction and historical survey

Let us consider rational languages X and Y, subsets of the free monoid A^* and their product

$$XY = \{ xy \in A^* \mid x \in X \text{ and } y \in Y \}.$$

In this lecture we wish to argue that this innocently looking operation is the source of much research and of some still unsolved problems, even though considerable progress has been achieved in the last decades, revealing many links between the Theory of Finite Automata and other fields of Mathematics.

The correct perspective to lead to our problem areas is from Kleene's theorem, so let us recall this cornerstone of the Theory of Finite Automata [17, 9].

Theorem 1 *For any finite alphabet A,* $\operatorname{Rec} A^* = \operatorname{Rat} A^*$.

Here, $\operatorname{Rec} A^*$ is the family of recognizable subsets of A^*, i.e. the ones recognized by (not necessarily deterministic) finite automata, while $\operatorname{Rat} A^*$ is the family of rational subsets of A^*, i.e. the least family of languages over A which contains the singleton sets $\{ a \}$, for $a \in A$, and is closed under union, product and star.

The terms of Kleene's theorem are nondeterministic in nature. Indeed, $\operatorname{Rec} A^*$ was defined in terms of nondeterministic automata, even though we know that any set in $\operatorname{Rec} A^*$ is recognized by a deterministic automaton. The nondeterministic setting for $\operatorname{Rec} A^*$ is, however, the correct one since it is in this form

* This work was done with partial support from FAPESP, CNPq and BID/USP.

that Kleene's theorem generalizes to the case of multiplicities in any semiring in place of the Boolean semiring. The interested reader can find the details in Eilenberg's book [9]; we only note that we will make use of the multiplicity theory in section 4. On the other side of Kleene's equation we find $\mathrm{Rat}\, A^*$ which is also nondeterministic, in the sense that any given rational language is denoted by an infinity of rational expressions, i.e. there are different ways of obtaining a set using the rational operations. This will be our starting point, since all three problems we will address began with questions about the existence or the optimization of expressions, possibly of restricted forms, to denote a given rational language.

Historically, the first problem of our interest, related to the product, was posed by R. McNaughton in 1960 [25] and solved by M. P. Schützenberger in 1965 [36] in the first real breakthrough in the area. Very interesting historical remarks about the formulation of the star-height problem can be found throughout the monograph of McNaughton and Papert [27], especially on page 99.

Let us recall first that every recognizable set is recognized by some *deterministic* automaton; it immediately follows that the family $\mathrm{Rec}\, A^*$, hence also $\mathrm{Rat}\, A^*$, is closed under complementation.[2] McNaughton's question was to characterize the family of star-free languages, i.e. the ones which can be expressed using only the singletons and the operations of union, complement and product. For instance, consider the language[3] $L = (ab + ba)^*$. Even though the star is used in this particular expression for L it can also be expressed without the star, hence it is a star-free language. We leave it to the reader the interesting exercise of verifying that the following expressions define L over the alphabet $A = \{ a, b \}$.[4]

$$I = A^* = \overline{\emptyset},$$

$$J = (ab)^* = 1 + aI \cap Ib \cap \overline{IaaI} \cap \overline{IbbI},$$

$$L = (ab + ba)^* = \overline{\overline{Iab}J\overline{aI} + \overline{Ib}Ja\overline{bI}}$$

In section 2 we will return to the star-free question, state Schützenberger's theorem and comment its many consequences.

The next problem to appear was Eggan's star-height problem. The *star-height of a rational expression* is the maximum number of nested stars in it. For instance, the star-height of

$$a^*b + ((ab^*)c)^* + (((a^*b + c)^* + d)^*e$$

is three. We define the *star-height of a set* X as being the least star-height of rational expressions denoting X. The star-height problem consists in determining

[2] Note that this statement about $\mathrm{Rat}\, A^*$ is an algebraic property of an algebraically defined family. However, its proof goes through Kleene's theorem and uses the concept of a *finite* automaton, which, in principle, has nothing to do with the family $\mathrm{Rat}\, A^*$.

[3] We frequently denote a union by $X + Y$; the empty word is denoted by 1.

[4] Unfortunately, there are no methods to produce beautiful symmetric expressions for star-free languages as in our example. This problem probably merits further study.

the star-height of a given rational language X. This problem, formulated in 1963 has been shown to be algorithmically decidable by Hashiguchi in 1988 [15] but, unfortunately no practically executable algorithm is known to determine the star height of a given set. We shall say more about this problem and some of the tools used to attack it in section 4.

Connected to the star-height problem we mention another problem of Brzozowski, formulated in 1966, which had a great influence in the theory. A language X has the *finite power property* if its star is the union of finitely many of its powers, i.e. if there exists an $m \geq 0$, such that $X^* = (1+X)^m$. This is equivalent to saying that

$$X^* = 1 + X + X^2 + \cdots + X^m.$$

This problem, solved independently by Hashiguchi [12] and the author [40] was the starting point for further developments which ultimately led to Hashiguchi's solution of the star-height problem. Note that Brzozowski's condition is sufficient in order to replace a star by finitely many unions and products.

Interested in star-free languages and inspired by Eggan's star-height hierarchy, J. A. Brzozowski formulated the dot-depth problem in the late 60's [8] which is, in general, still unsolved, despite the combined efforts of many researchers. The *dot-depth of a star-free rational expression* is the maximum nested levels of concatenation used in the expression. The *dot-depth of a language* is the least dot-depth of star-free expressions denoting it. The dot-depth problem asks for the characterization of languages of any given dot-depth. For instance the previous star-free expressions show that the dot-depths of A^*, $(ab)^*$ and $(ab+ba)^*$ are at most 0, 1 and 2, respectively. However, it is a nontrivial journey to prove that 2 *is* the dot-depth of $(ab+ba)^*$ [38].

The dot-depth problem has an easy solution for dot-depth zero. The next step, i.e. the characterization of dot-depth one languages was achieved by R. Knast in 1983 [18]. For depth two or more the problem is open, but important partial results of Margolis, Pin, Straubing and Weil in that direction should be mentioned. We leave the details to section 3.

We close this introduction by mentioning that the first and third problems here described led to the discovery of many interesting families of rational languages, called varieties. The study of these varieties is mathematically sophisticated and it combines algebraic, combinatorial, logical and lately topological methods to attack linguistic problems. Reciprocally, linguistic properties are often used to establish algebraic results about pseudovarieties. Such mathematical diversity and richness is one of the main credentials of this theory. Extensive and modern accounts of these developments can be found in the books of Pin [31] and Almeida [3].

2 More on McNaughton's star-free problem

McNaughton's question on star-free languages was not motivated by its linguistic aspect but it appeared as a natural question related to the representation of rational languages by logical formulas. This area was pioneered by Trakhtenbrot

[56] and independently discovered by McNaughton [25]. See also the fundamental work of Büchi [7] and Elgot [11].

More precisely, following Büchi, rational languages can be defined by formulas in the monadic second order theory of successor. A restriction to first order formulas leads to the subfamily of star-free languages and this was the original motivation of McNaughton for his interest in star-free languages. The reader will find further details in [27, 51, 54, 28].

Now we recall that every language X has a syntactic monoid M and a syntactic morphism $f\colon\ A^* \to M$ which have the property that $f^{-1}fX$ equals X. Furthermore, M is the least monoid with this property in the sense that for every other morphism $f'\colon\ A^* \to M'$, such that $f'^{-1}f'X = X$, M is a homomorphic image of M'. We will say that a monoid M is *aperiodic* if for every $x \in M$ there exists an $n > 0$, such that $x^n = x^{n+1}$. Here is Schützenberger's theorem.

Theorem 2 *A set X in* $\operatorname{Rat} A^*$ *is star-free iff the syntactic monoid of X is finite and aperiodic.*

We wish to comment now on three aspects of Schützenberger's paper [36] containing this theorem:

- the effective solution of a linguistic problem through the use of the syntactic monoid;
- the introduction of the Schützenberger product for finite monoids;
- the lead it contained for the introduction and investigation of pseudovarieties, one of the most significant aspects of the theory today.

Let us examine first the constructive aspect of Schützenberger's solution of the star-free problem. Note that the syntactic monoid can be constructed algorithmically for a recognizable set, given an automaton recognizing it or an expression denoting it. Since one can easily check whether the syntactic monoid of a language is aperiodic or not it follows that the theorem is an effective characterization of star-free sets. This is one of the theorem's major aspects, certainly the one which motivated McNaughton's question. Maybe it even stimulated and justified the study of the syntactic monoid. Indeed, this invariant has been known for a long time and both Schützenberger and Rhodes were directing some of the work of their respective schools to the investigation of these algebraic structures since the beginning of their activity. However, the structure only gained widespread acceptance after the appearance of Schützenberger's theorem, effectively characterizing star-free languages.

Next we comment on the Schützenberger product of monoids. Note that given languages X and Y, the syntactic monoid of $X + Y$ divides the direct product of the syntactic monoids of X and Y. One of the difficulties in handling the product of languages, our main concern here, is that we do not have a simple operation on monoids which would play the role of the direct product in the above statement. Such a product was introduced during the course of the original proof of theorem 2. This product is now called the Schützenberger product and it can be found in section 5.

The product was originally defined for two monoids. Straubing took this idea of the 2-fold Schützenberger product and generalized it for a k-fold product. His definition can be found in section 5. This was an essential step because the Schützenberger product is not associative and the iterated use of the 2-fold product introduces unnecessary and unwanted algebraic "complexities". Next, Straubing proved that the Schützenberger product is an operation on monoids which reflects the (k-fold) product of languages in the sense mentioned before. On the other hand, Reutenauer proved in 1979 [34] an inverse result for the 2-fold Schützenberger product, using the marked product of languages. More precisely, he proved that every language recognized by the 2-fold Schützenberger product of monoids M_1 and M_2 can be expressed as a Boolean combination of marked products $L_1 a L_2$, where L_i is recognized by M_i and a is a letter. Pin generalized this proof and showed [29] a similar property for the k-fold product. From all these developments we can conclude that the Schützenberger product is the monoid equivalent of the marked product of languages. This transforms the Schützenberger product in a major tool to attack product problems for rational languages. In section 5 we give a full proof of this basic property of the Schützenberger product, and this will be the only proof in our paper.

The last aspect we will comment is still another far reaching consequence of Schützenberger's work. It provides perhaps the earliest example of a pseudovariety of monoids, theme which dominates the modern research in the area.

A pseudovariety of monoids is a class of finite monoids which is closed under formation of submonoids, of homomorphic images and of finite direct products. These classes are the finite analogue of Birkhoff's varieties of algebras which are exactly the classes of algebras definable by equations. An example of a pseudovariety of monoids is given by the class $\mathbf{A}$ of finite aperiodic monoids. Schützenberger noted very early this connection [37] but the subject was to be developed only in the book of Eilenberg [10] in 1976. One problem is that on account of the finiteness the equational property of varieties, present in Birkhoff's theorem, is lost, i.e. it is not true that every pseudovariety is the class of finite monoids satisfying some set of equations. Nevertheless, Eilenberg and Schützenberger have shown [10] that the equational property can be partially recovered. Indeed, they proved that every pseudovariety of monoids is ultimately defined by equations. Another, very elegant proof of this fine theorem was found by Ash [4]. Let us illustrate this property by the example of $\mathbf{A}$. Consider the equation $x^n = x^{n+1}$, one for every $n \geq 1$. It is easy to see that only the idempotent monoids, in which $x = x^2$, satisfy *all* of these equations. It is equally easy to see that every aperiodic monoid satisfies all but finitely many of these equations: it is said therefore that those equations *ultimately define* the class $\mathbf{A}$.

Later on, Reiterman [33] improved the analogy with Birkhoff's theorem by introducing the topological algebra of the implicit operations on finite monoids (finite algebras in general). He proved that every pseudovariety is defined by pseudoidentities. For the case of $\mathbf{A}$, the pseudoidentity defining it is $x^\omega = xx^\omega$, where x^ω is a typical example of an implicit operation which is not a homomorphism. It associates to each element x of a monoid its unique power x^ω which is idempotent. The use and calculus of implicit operations for pseudovarieties of monoids was significantly developed by Jorge Almeida who recently wrote a comprehensive book about the subject [3]. This area still has many unanswered and interesting questions, the book of Almeida, for instance, lists 57 open problems.

3 More on Brzozowski's dot-depth problem

We begin with a precise linguistic statement of the dot-depth problem. For technical reasons we will initially restrict our attention to languages which do not contain the empty word, i.e. our universe for languages will be 2^{A^+}, for a fixed alphabet A. Let $\mathcal{E}$ be the family of singletons, one for each letter of A. For a family $\mathcal{F}$ of languages we denote by $\mathcal{BF}$ the smallest Boolean algebra containing $\mathcal{F}$, i.e. the closure of $\mathcal{F} \cup \{\emptyset\}$ under union and complementation. Let us denote by $\mathcal{SF}$ the smallest semigroup containing $\mathcal{F}$, i.e. the closure of $\mathcal{F}$ under multiplication. The dot-depth hierarchy is the sequence

$$\mathcal{B}_0 \subseteq \mathcal{B}_1 \subseteq \cdots \subseteq \mathcal{B}_n \subseteq \cdots$$

of Boolean algebras, where $\mathcal{B}_0 = \mathcal{BE}$ and $\mathcal{B}_{n+1} = \mathcal{BSB}_n$, for $n \geq 0$. Now, we say that a language $L \subseteq A^*$ is of *dot-depth* n if $L - \{1\}$ belongs to $\mathcal{B}_n$ but not to $\mathcal{B}_{n-1}$. The dot-depth problem consists in (effectively) characterizing the languages of each given dot-depth.

The idea here is to minimize the nested number of levels of concatenation in expressions denoting the star-free sets: $\mathcal{B}_n$ is the family of star-free languages which must use n nested levels of concatenation and for which that many levels are sufficient to denote them. Clearly, each $\mathcal{B}_n$ is a subfamily of the star-free sets, and each star-free set belongs to some $\mathcal{B}_n$, but not much more than this follows by intuitive arguments.

It can be shown without difficulty that each $\mathcal{B}_n$ is a $+$-variety of languages, in the terminology of Eilenberg [10], and this essentially means that the syntactic semigroups of languages in $\mathcal{B}_n$ form exactly the syntactic semigroups of some pseudovariety of semigroups. The corresponding pseudovariety of semigroups will be denoted by $\mathbf{B}_n$.

It is known that the hierarchy is proper but the proof of this result already requires sophisticated arguments. It was first proved by Brzozowski and Knast in 1978 [5]. A more informative and algebraic proof was later obtained by Straubing [46]. Another proof, logically oriented, was given by Thomas [52, 53].

Straubing proved initially that $\mathbf{B}_{n+1} = \Diamond\mathbf{B}_n$, where $\Diamond\mathbf{V}$ is the pseudovariety generated by the Schützenberger product of semigroups in $\mathbf{V}$. Straubing's proof of the properness of the dot-depth hierarchy was done then by a careful analysis of the algebraic properties of the Schützenberger product of semigroups.

As for the dot-depth problem the strongest known result is the characterization of dot-depth one languages, achieved by Knast [18]. Knast's condition is a bit complicated to be stated here; we only mention that it is an effective property on the syntactic semigroup of a language which gives a necessary and sufficient condition for a language to be of dot-depth one. The same problem for dot-depth two is still open, despite the many efforts of solving it. The closest results so far were obtained by Straubing and Weil in a series of papers [48, 58, 50]. Another line of attack tried to characterize the power operator **P**, since an effective characterization of **PJ** would solve the problem [45, 22, 32, 23, 24, 30, 1].

At this point we mention some early results on the dot-depth problem which had an influence on the forthcoming research in this area. These are contained in the Doctoral dissertation of the author [38], written in 1972. Three problems were tackled there: the characterization of locally testable languages, the characterization of piecewise testable languages and the localization of two infinite hierarchies of languages of dot-depth one.

A language X is said to be *locally testable* if pertinence of a word to X can be decided by looking only at segments of bounded length of the given word. The problem of effectively characterizing locally testable languages has been formulated by McNaughton and Papert in their monograph [27] and it was solved independently by McNaughton and by Brzozowski and Simon [26, 6]. It is easy to see that a language is locally testable iff it belongs to the Boolean algebra generated by the sets A^*wA^*, A^*w and wA^*, for words w. This clearly implies that every locally testable language is of dot-depth one.

Theorem 3 *A subset of A^* is locally testable iff its syntactic semigroup S is finite and locally idempotent and commutative, i.e. for every idempotent $e = e^2$ in S the monoid eSe in S is idempotent and commutative.*

One of the major steps in our solution corresponded to a wreath-product decomposition of semigroups which are locally idempotent and commutative and which became known as "A theorem on graphs", after its reformulation by Eilenberg [10]. This result inspired Knast to obtain a technically more complex theorem on graphs [19] and which allowed him to characterize the whole family of languages of dot-depth one[18]. Later on, starting from these theorems on graphs, Tilson developed the Theory of Finite Categories as Algebras [55], as a generalization of the Theory of Finite Monoids and which is bound to play a crucial role in a possible solution of the dot-depth problem. Another very important result in this area is contained in the $\mathbf{V} * \mathbf{D}$ paper [47] of Straubing; theorem 3 is also the first discovered particular case of Straubings results on $\mathbf{V} * \mathbf{D}$.

A language X is *piecewise testable* if pertinence of a word to X can be decided by looking at subwords of bounded length of the given word. Note that $u = a_1a_2 \cdots a_n$, with $a_i \in A$, is a *subword* of v iff $v \in A^*a_1A^* \cdots a_nA^*$. This last set is the shuffle product of u and A^*, denoted $u \sqcup A^*$. It is easy to see that a language is piecewise testable iff it belongs to the Boolean algebra generated by the sets $u \sqcup A^* = A^*a_1A^* \cdots a_nA^*$. Piecewise testable languages were first considered by the author [38, 39] who also obtained several characterizations. The most important one is the following.

Theorem 4 *A subset of A^* is piecewise testable iff its syntactic monoid is finite and $\mathcal{J}$-trivial.*

We recall that a monoid M is $\mathcal{J}$-trivial iff every principal ideal of M has a unique generator. In other words, for any $m_1, m_2 \in M$, $Mm_1M = Mm_2M$ implies that $m_1 = m_2$. This is an important structural property of monoids and the corresponding pseudovariety $\mathbf{J}$ appears frequently especially in connection with the Schützenberger product and the dot-depth problem. Note, as a starter, that the shuffle product $u \sqcup A^*$ is a particular case (perhaps the simplest one) of the marked product of section 5.

The family of piecewise testable sets possesses today many characterizations, some of them having more than one proof. We do not have space to review these here but indicate some of the literature [10, 35, 44, 49, 2]. Perhaps the most outstanding proof so far is that of Almeida which contains a completely topological proof of theorem 4 staged in Universal Algebraic terms. Even though his proof is not constructive it yields an effective decision procedure for the problem of deciding whether or not a given recognizable set is piecewise testable.

The third aspect we mentioned was the identification of two infinite hierarchies inside $\mathcal{B}_1$, particular families of which were the locally testable languages and the piecewise testable ones. Again, we will not survey this aspect here and only mention that this subject was much expanded by Pin who in [29] introduced a formalism to construct many hierarchies inside the family of star-free sets and which are very closely related to the role of the Schützenberger product in the theory of pseudovarieties (see section 5). We even believe that a proper study of the algebraic properties of the hierarchies introduced by Pin might lead to a solution of the dot-depth problem.

4 More on Eggan's star-height problem

Instead of addressing the star-height problem in detail we shall try to describe here only the main tool developed to deal with this problem area, pointing out its connection with the product of rational languages. Even this we will do very briefly, a more detailed account can be found in our survey [41].

Consider initially the following problem. Let be given a finite family $\mathcal{F}$ of rational languages. Can we decide whether a given language, L belongs to the closure of $\mathcal{F}$ under certain operations? Hashiguchi solved this problem in 1983 for any subset of the rational operations: union, product and star [14]. Two cases are particularly interesting and difficult: the closure of $\mathcal{F}$ under product and its closure under union and product. Representing the elements of $\mathcal{F}$ by $X_1, X_2, \ldots, X_n$, in the first case we wish to know whether some monomial in the (noncommuting) X's (i.e. a product $X_{i_1} X_{i_2} \cdots X_{i_k}$) denotes L. In the second case one is interested in a polynomial in the X's, denoting L. But what is the relation to the star-height problem? Consider the following situation: we have already found expressions of star-height at most h for the sets X_i. We are given the language L. Can we express L^* as unions of products of the X_i's? If so, then we can guarantee that the height of L^* is at most h. This technique alone is not strong enough to solve Eggan's problem but it does describe an important aspect of Hashiguchi's solution.

We shall consider now the particular case of these problems when there is only one language in $\mathcal{F}$, or equivalently, there is only one variable X and the set to be expressed is X^*. Recall the definition of the finite power property, given in the Introduction, and note that the solution to either problem above (for one variable) can be expressed in terms of the finite power property for the only language in $\mathcal{F}$. This problem is already quite difficult and it will illustrate well the general case.

The problem of deciding whether or not a rational language has the finite power property was first formulated by J. A. Brzozowski in 1966 during the seventh SWAT (now FOCS) Conference. It was solved independently by Hashiguchi [12] and the author [40]. Our solution introduced the theory of multiplicities over the tropical semiring[5] (see [41]) which seems to be an important tool in minimizing the number of factors in expressions involving products of rational languages. We try to illustrate the idea briefly by an example.

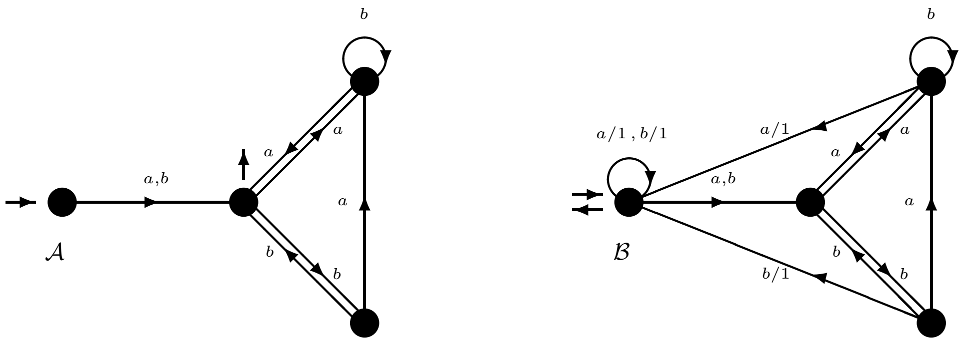

Fig. 1. A set X with the finite power property: $X^* = (1 \cup X)^4$.

Consider the language L recognized by the automaton $\mathcal{A}$ of Figure 1. Automaton $\mathcal{B}$ (without the multiplicities /1) is the automaton recognizing the language L^*, obtained by a standard construction; let i be its only initial and final state. Let us now assign a multiplicity 1 to each edge arriving at the final state i of $\mathcal{B}$ and multiplicity 0 to every other edge of $\mathcal{B}$ (zero multiplicities are not indicated in the figure). Let us postulate that the multiplicity of a path is the sum of multiplicities of its edges. The multiplicity of a word w is the least multiplicity of successful paths spelling w. These rules are easily remembered if one interprets the multiplicities as a "cost". Now, every $i - i$ path in $\mathcal{B}$, spelling $w \in L^*$, induces a factorization of w showing that $w \in L^n$, where n is the multiplicity of our path. It follows that the multiplicity of every word w in the behavior of $\mathcal{B}$ is

[5] This is the semiring consisting of the natural numbers extended with ∞ and equipped with the operations of minimums (as semiring addition) and addition (as semiring product).

the least exponent n, such that L^n contains w. Finally, the set L has the finite power property iff the words in L^* have bounded multiplicity. Or equivalently, iff the behavior of $\mathcal{B}$ is *limited*.

The last problem, deciding whether or not the behavior of an arbitrary finite automaton is limited is a basic ingredient in the solution of the star-height problem and many other related problems. It is a hard problem, first solved by Hashiguchi [13] and which since then has given rise to much research [21, 43, 42, 16, 57] which description is out of the scope of this paper.

We mention a recent result of D. Krob [20] which surprised everyone in the area. Krob has proved that the equivalence problem for finite automata with multiplicities in the tropical semiring is recursively undecidable. He did this by a very ingenious construction which solved Hilbert's tenth problem using only the very rudimentary arithmetic available in the tropical semiring and the equally rudimentary computing powers of finite automata. With such limited resources he was able to express the multiplication of natural numbers. Thus, Krob proved the undecidability of the equivalence problem using a reduction from Hilbert's tenth problem.

5 Languages of the Schützenberger product of monoids

In this section we prove a theorem incorporating work of Schützenberger, Straubing, Reutenauer and Pin [36, 46, 34, 31]. This result is one of the most important tools to work with products of rational languages. Our proof is a major simplification of earlier ones and is reminiscent of some of the early linguistic proofs related to the dot-depth problem. In a forthcoming paper we intend to explore the possible benefits of such a transparent proof.

Theorem 5 *Let A be a finite alphabet and let $M_0, M_1, \ldots, M_n$ be finite monoids. Then $\Diamond = \Diamond(M_0, M_1, \ldots, M_n)$ recognizes a language $L \subseteq A^*$ iff L can be expressed as a Boolean combination of languages of the form*

$$L_{i_0} a_1 L_{i_1} \cdots a_r L_{i_r}, \tag{1}$$

where $0 \leq r \leq n$, $0 \leq i_0 < i_1 < \cdots < i_r \leq n$, $a_i \in A$ (for $1 \leq i \leq r$), and $L_{i_j} \subseteq A^*$ is a language recognized by M_j (for $0 \leq j \leq r$).

Initially we give precise definitions of the terms of theorem 5. Let us consider monoids $M_0, M_1, \ldots, M_n$ and let $M = M_0 \times M_1 \times \cdots \times M_n$ be their direct product. The family K of subsets of M is a semiring under the operations of union and product of subsets of M. The *Schützenberger product* of the M_i's, denoted $\Diamond(M_0, M_1, \ldots, M_n)$, is the semigroup of $(n+1) \times (n+1)$ matrices $P = (P_{ij})$ over K whose elements satisfy the following properties:

1. $P_{ij} = \emptyset$, for every $0 \leq j < i \leq n$;
2. $P_{ij} \subseteq 1 \times \cdots \times 1 \times M_i \times \cdots \times M_j \times 1 \cdots \times 1$, for every $0 \leq i \leq j \leq n$;
3. P_{ii} is a unitary subset of K, for every $0 \leq i \leq n$.

For a monoid M and a language $L \subseteq A^*$ we say that M *recognizes* L if there exists a morphism $\mu\colon A^* \to M$ such that $L = f^{-1}fL$.

Lemma 6 *Every language of the form (1) is recognized by* $\diamond$.

Proof. Initially we note that $\diamond(M_{i_0}, \dots, M_{i_r})$ is a submonoid of $\diamond(M_0, \dots, M_n)$; hence, there is no loss of generality if we assume that the language to be recognized is $L = L_0 a_1 L_1 \cdots a_n L_n$, where L_i is recognized by M_i. Assume that $\mu_i\colon A^* \to M_i$ are morphisms, for $0 \le i \le n$, such that μ_i recognizes the language L_i, i.e. $L_i = \mu^{-1}\mu L_i$. We define matrices $a\mu$, for $a \in A$, as follows:

$$(a\mu)_{pq} = \begin{cases} (1, \dots, 1, \mu_p a, 1, \dots, 1) & \text{if } p = q; \\ (1, \dots, 1) & \text{if } a = a_p \text{ and } q = p+1; \\ \emptyset & \text{else.} \end{cases}$$

Considering the unique extension of μ to a morphism, $\mu\colon A^* \to \diamond$, we have, for every $w \in A^*$,

$$(w\mu)_{pq} = \begin{cases} (1, \dots, 1, \mu_p w, 1, \dots, 1) & \text{if } p = q; \\ \{\, (1, \dots, 1, \mu_p w_p, \dots, \mu_q w_q, 1, \dots, 1) \mid w \in A^* w_p \cdots a_q w_q A^* \,\} & \text{if } p \ne q. \end{cases}$$

Thus, assuming that subset X_i of M_i is such that $L_i = \mu_i^{-1} X_i$, we have that $L = \mu^{-1} X$, where

$$X = \{\, P \in \diamond(M_0, \dots, M_n) \mid P_{0n} \cap X_0 \times \cdots \times X_n \ne \emptyset \,\}.$$

■

To show the other implication in theorem 5 we consider a language $L \subseteq A^*$ recognized by $\diamond$ and a morphism $\mu\colon A^* \to \diamond$, such that $L = \mu^{-1}\mu L$. We shall study the morphism μ in detail. Initially, we define functions $\mu_{ij}\colon A^* \to K$ by putting $\mu_{ij} x = (\mu x)_{ij}$. Note that, for each $0 \le i \le n$, μ_{ii} is a morphism, which is easily identified with a morphism $A^* \to M_i$, but no similar property holds for the μ_{ij} in general. The next lemma says that μ_{ij} is essentially computed by the morphisms μ_{kk}. It contains the inspiration for our proof.

Lemma 7 *For every word* $w \in A^*$, *and for every* $0 \le i, j \le n$,

$$\mu_{ij} w = \sum \mu_{i_0 i_0} w_{i_0} \mu_{i_0 i_1} a_1 \mu_{i_1 i_1} w_{i_1} \cdots \mu_{i_{k-1} i_k} a_k \mu_{i_k i_k} w_{i_k},$$

where the sum extends over all $0 \le k \le n$, *all* $i = i_0 < i_1 < \cdots < i_k = j$, *and all factorizations* $w = w_{i_0} a_1 w_{i_1} \cdots a_k w_{i_k}$, *with* $a_i \in A$.

Proof. Let $w = b_1 b_2 \cdots b_r$ be the factorization of w in letters. The nature of matrix multiplication guarantees that

$$\mu_{ij} w = \sum \mu_{i_0 i_1} b_1 \mu_{i_1 i_2} b_2 \cdots \mu_{i_{r-1} i_r} b_r,$$

where the sum extends over all $i = i_0, i_1, \dots, i_r = j$. Since $\mu_{pq} x = \emptyset$, whenever $p > q$, it is enough to consider sequences such that $i = i_0 \le i_1 \le \cdots \le i_r = j$.

Grouping now equal neighboring indices and remembering that each μ_{kk} is a morphism we arrive at the desired expression for $\mu_{ij}w$. ∎

This lemma suggests the following definition, crucial in the proof. An *object* is a sequence

$$o = (i_0, m_0, a_1, i_1, m_1, \ldots, a_k, i_k, m_k),$$

where $0 \le k \le n$, $0 \le i_0 < i_1 < \cdots < i_k \le n$, $a_i \in A$ and $m_j \in M_{i_j}$. Integer k is the *length* of the object o. There are finitely many objects and $\mathcal{O}$ will denote the set of all of them. Given μ we define the *value* of o as being

$$f(o) = m_0(\mu_{i_0 i_1} a_1)m_1 \cdots (\mu_{i_{k-1} i_k} a_k)m_k,$$

and do note that $f(o) \subseteq 1 \times \cdots \times 1 \times M_{i_0} \times \cdots \times M_{i_k} \times 1 \times \cdots \times 1$. For $u \in A^*$ we define its *contents* by

$$\mathrm{cont}(u) = \{\, o \in \mathcal{O} \mid u = u_0 a_1 u_1 \cdots a_k u_k, \text{ with } \mu_{i_j i_j} u_j = m_j, \text{ for each } j \,\},$$

i.e. the contents of u consists of those objects for which u has a compatible factorization. Finally we define an equivalence relation, $\equiv \bmod \Diamond$, by

$$u \equiv v \bmod \Diamond \text{ iff } \mathrm{cont}(u) = \mathrm{cont}(v).$$

The reader will verify at once that $\equiv \bmod \Diamond$ is a congruence relation over A^* since $\mathrm{cont}(ua)$, for $a \in A$, depends only on $\mathrm{cont}(u)$ and a, but not on u itself. Besides, since there are only finitely many objects, we can conclude that $\equiv \bmod \Diamond$ is a congruence of finite index. We will denote by F_μ the quotient monoid $A^*/\equiv \bmod \Diamond$ and by π the natural projection $\pi\colon A^* \to F_\mu$.

Corollary 8 *The congruence $\pi^{-1}\pi$ is a refinement of the congruence $\mu^{-1}\mu$, i.e., $\pi^{-1}\pi \subseteq \mu^{-1}\mu$.*

Proof. Observe initially that from Lemma 7 we can conclude that for every $u \in A^*$ and $0 \le i, j \le n$, $\mu_{ij}u$ depends only on $\mathrm{cont}(u)$ and not on u itself. Assume that $u \equiv v \bmod \Diamond$. It follows that $\mu u = \mu v$. The proof is complete. ∎

Now we are ready to prove the second part of theorem 5.

Lemma 9 *Every language recognized by $\Diamond$ belongs to $\mathcal{F}$, where $\mathcal{F}$ is the family of Boolean combinations of languages of the form (1).*

Proof. Every language recognized by $\Diamond$ is a finite union of congruence classes $\mu^{-1}\mu$. Thus, it suffices to show that each such class is in $\mathcal{F}$.

Since $\pi^{-1}\pi$ is of finite index, in view of Cor. 8 each congruence class $\mu^{-1}\mu$ is a finite union of congruence classes of $\pi^{-1}\pi$. Hence, it suffices to show that each congruence class of $\pi^{-1}\pi$ is in $\mathcal{F}$. To do this, we associate a language $L(o)$ to every object o as follows:

$$L(o) = \{\, u \in A^* \mid o \in \mathrm{cont}(u) \,\}.$$

Recalling the definition of an object and that each μ_{ii} is a morphism it is easy to see that

$$L(o) = (\mu_{i_0 i_0}^{-1}\mu_{i_0 i_0} m_0) a_1 (\mu_{i_1 i_1}^{-1}\mu_{i_1 i_1} m_1) \cdots\ a_k (\mu_{i_k i_k}^{-1}\mu_{i_k i_k} m_k).$$

Thus, $L(o)$ is of the form (1) and consequently belongs to $\mathcal{F}$.

We observe now that, for every $u \in A^*$,

$$\pi^{-1}\pi u = \bigcap_{o \in \mathrm{cont}(u)} L(o) - \bigcup_{o \in \mathcal{O} - \mathrm{cont}(u)} L(o).$$

It follows that each congruence class $\pi^{-1}\pi u$ is in $\mathcal{F}$ and this concludes the proof of the Lemma. ∎

Theorem 5 is established now by lemmas 6 and 9.

References

1. J. Almeida. On power varieties of semigroups. *J. Algebra*, 120:1–17, 1989.
2. J. Almeida. Implicit operations on finite $\mathcal{J}$-trivial semigroups and a conjecture of I. Simon. *J. Pure Appl. Algebra*, 69:205–218, 1990.
3. J. Almeida. *Semigrupos Finitos e Álgebra Universal.* IME-USP, São Paulo, 1992. in portuguese.
4. C. J. Ash. Pseudovarieties, generalized varieties and similarly described classes. *J. Algebra*, 92:104–115, 1985.
5. J. A. Brzozowski and R. Knast. The dot-depth hierarchy of star-free languages is infinite. *J. Comput. Syst. Sci.*, 16:37–55, 1978.
6. J. A. Brzozowski and I. Simon. Characterizations of locally testable events. *Discrete Math.*, 4:243–271, 1973.
7. J. R. Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundlagen Math.*, 6:66–92, 1960.
8. R. S. Cohen and J. A. Brzozowski. Dot-depth of star-free events. *J. Comput. Syst. Sci.*, 5:1–15, 1971.
9. S. Eilenberg. *Automata, Languages, and Machines, Volume A.* Academic Press, New York, 1974.
10. S. Eilenberg. *Automata, Languages, and Machines, Volume B.* Academic Press, New York, 1976.
11. C. C. Elgot. Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc.*, 98:21–52, 1961.
12. K. Hashiguchi. A decision procedure for the order of regular events. *Theoretical Comput. Sci.*, 8:69–72, 1979.
13. K. Hashiguchi. Limitedness theorem on finite automata with distance functions. *J. Comput. Syst. Sci.*, 24:233–244, 1982.
14. K. Hashiguchi. Representation theorems on regular languages. *J. Comput. Syst. Sci.*, 27:101–115, 1983.
15. K. Hashiguchi. Algorithms for determining relative star height and star height. *Information and Computation*, 78:124–169, 1988.
16. K. Hashiguchi. Improved limitedness theorems on finite automata with distance functions. *Theoretical Comput. Sci.*, 72, 1990.

17. S. C. Kleene. Representations of events in nerve nets and finite automata. In Shannon, editor, *Automata Studies*, pages 3–41. pup, princeton, 1956.
18. R. Knast. A semigroup characterization of dot-depth one languages. *R.A.I.R.O. Informatique Théorique*, 17:321–330, 1983.
19. R. Knast. Some theorems on graph congruences. *R.A.I.R.O. Informatique Théorique*, 17:331–342, 1983.
20. D. Krob. The equality problem for rational series with multiplicities in the tropical semiring is undecidable. *Int. J. of Algebra and Computation*, 1993. in print.
21. H. Leung. On the topological structure of a finitely generated semigroup of matrices. *Semigroup Forum*, 37:273–287, 1988.
22. S. W. Margolis. On M-varieties generated by power monoids. *Semigroup Forum*, 22:339–353, 1981.
23. S. W. Margolis and J.-E. Pin. Minimal noncommutative varieties and power varieties. *Pacific J. Math.*, 111:125–135, 1984.
24. S. W. Margolis and J.-E. Pin. Power monoids and finite $\mathcal{J}$-trivial monoids. *Semigroup Forum*, 29:99–108, 1984.
25. R. McNaughton. Symbolic logic for automata. Technical Report Tech. Note No. 60-244, Wright Air Development Division, Cincinnati, Ohio, 1960.
26. R. McNaughton. Algebraic decision procedures for local testability. *Math. Syst. Theor.*, 8:60–76, 1974.
27. R. McNaughton and S. Papert. *Counter-Free Automata*. The M.I.T. Press, Cambridge, Mass., 1971.
28. D. Perrin and J.-E. Pin. First-order logic and star-free sets. *J. Comput. Syst. Sci.*, 32:393–406, 1986.
29. J.-E. Pin. Hiérarchies de cocaténation. *R.A.I.R.O. Informatique Théorique*, 18:23–46, 1984.
30. J.-E. Pin. Semigroupe des parties et relations de Green. *Can. J. Math*, 36:327–343, 1984.
31. J.-E. Pin. *Variétés de Langages Formels*. Masson, Paris, 1984. English translation: Varieties of Formal Languages, Plenum, 1986.
32. J.-E. Pin and H. Straubing. Monoids of upper triangular matrices. In *Colloquia Mathematica Societatis Janos Bolyai, 39, Semigroups*, pages 259–272, Szeged, 1981.
33. J. Reiterman. The Birkhoff theorem for finite algebras. *Alg. Univ.*, 14:1–10, 1982.
34. C. Reutenauer. Sur les variétés de langages et de monoïdes. In *GI 79*, pages 260–265, Berlin, 1979. Springer-Verlag. Lecture Notes in Computer Science, 67.
35. J. Sakarovitch and I. Simon. Subwords. In M. Lothaire, editor, *Combinatorics on Words*, pages 105–144. Addison-Wesley, Reading, MA, 1983. Encyclopaedia of Mathematics, volume 17.
36. M. P. Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8:190–194, 1965.
37. M. P. Schützenberger. Sur certaines variétés de monoïdes finis. In E. R. Caianello, editor, *Automata Theory*, pages 314–319. Academic Press, 1966.
38. I. Simon. *Hierarchies of Events with Dot-Depth One*. PhD thesis, University of Waterloo, Waterloo, Ont., Canada, 1972. Department of Applied Analysis and Computer Science.
39. I. Simon. Piecewise testable events. In H. Brakhage, editor, *Automata Theory and Formal Languages, 2nd GI Conference*, pages 214–222, Berlin, 1975. Springer-Verlag. Lecture Notes in Computer Science, 33.

40. I. Simon. Limited subsets of a free monoid. In *Proc. 19th Annual Symposium on Foundations of Computer Science*, pages 143–150, Piscataway, N.J., 1978. Institute of Electrical and Electronics Engineers.
41. I. Simon. Recognizable sets with multiplicities in the tropical semiring. In M. P. Chytil, L. Janiga, and V. Koubek, editors, *Mathematical Foundations of Computer Science 1988*, pages 107–120, Berlin, 1988. Springer-Verlag. Lecture Notes in Computer Science, 324.
42. I. Simon. On semigroups of matrices over the tropical semiring. Technical Report RT-MAC-8907, Departamento de Ciência da Computação do IME-USP, São Paulo, 1989.
43. I. Simon. Factorization forests of finite height. *Theoretical Comput. Sci.*, 72:65–94, 1990.
44. J. Stern. Characterizations of some classes of regular events. *Theoretical Comput. Sci.*, 35:17–42, 1985.
45. H. Straubing. Recognizable sets and power sets of finite semigroups. *Semigroup Forum*, 18:331–340, 1979.
46. H. Straubing. A generalization of the Schützenberger product of finite monoids. *Theoretical Comput. Sci.*, 13:137–150, 1981.
47. H. Straubing. Finite semigroup varieties of the form $V * D$. *J. Pure Appl. Algebra*, 36:53–94, 1985.
48. H. Straubing. Semigroups and languages of dot-depth two. *Theoretical Comput. Sci.*, 58:361–378, 1988.
49. H. Straubing and D. Thérien. Partially ordered finite monoids and a theorem of I. Simon. *J. Algebra*, 119:393–399, 1988.
50. H. Straubing and P. Weil. On a conjecture concerning dot-depth two languages. *Theoretical Comput. Sci.*, 104:161–183, 1992.
51. W. Thomas. Classifying regular events in symbolic logic. *J. Comput. Syst. Sci.*, 25:360–376, 1982.
52. W. Thomas. An application of the Ehrenfeucht-Fraissé game in formal language theory. *Soc. Math. France, 2e série*, 16:11–21, 1984.
53. W. Thomas. A concatenation game and the dot-depth hierarchy. In *Computation Theory and Logic*, pages 415–426, Berlin, 1987. Springer-Verlag. Lecture Notes in Computer Science, 270.
54. W. Thomas. Automata on infinite objects. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume B, Formal Models and Semantics*, chapter 4, pages 133–191. Elsevier, elsevierp, 1990.
55. B. Tilson. Categories as algebra: an essential ingredient in the theory of monoids. *J. Pure Appl. Algebra*, 48:83–198, 1987.
56. B. A. Trakhtenbrot. Synthesis of logic networks whose operators are described by means of single-place predicate calculus. *Doklady Akad. Nauk. SSSR*, 118:646–649, 1958. in russian.
57. A. Weber. Exponential upper and lower bounds for the order of a regular language. Technical report, Fachbereich Informatik, Johann Wolfgang Goethe-Universitä, Frankfurt, 1992.
58. P. Weil. Inverse monoids of dot-depth two. *Theoretical Comput. Sci.*, 66:233–245, 1989.