Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

An Hadamard operation on rational relations

Christian Choffrut

LIAFA, Université Paris Diderot – Paris 7 & CNRS, Case 7014 75205 Paris Cedex 13, France

ARTICLE INFO

Article history:
Received 22 February 2015
Received in revised form 22 October 2015
Accepted 29 October 2015
Available online xxxx

Keywords:
Finite automata
Binary rational relations on integers
Rational series
Hadamard product
Hadamard star
Decidability

ABSTRACT

We consider a new operation on the family of binary relations on integers called Hadamard star. View a binary relation $R \subseteq \mathbb{N} \times \mathbb{N}$ as a mapping of $\mathbb{N}$ into the power set of $\mathbb{N}$ and let $R(n)$ denote the subset of integers m such that $(n,m) \in R$. Then the Hadamard star of R is the relation which assigns to each integer n the Kleene star of $R(n)$. This is reminiscent of the Hadamard inverse of series with coefficients in a field.

We characterize the rational relations whose Hadamard star is also rational and show that this property is decidable.

1. Introduction

In 2013 I worked with Bruno Guillon on binary relations defined by unary two-way transducers which are finite state devices provided with one read-only two-way input tape and one write only one-way output tape. Input and output alphabets are unary. The difference with one-way transducers relies essentially upon the fact that along with the current state of the automaton one needs to record the position on the input word. In the one-way case, the computation is governed by determinants of matrices, whose dimension is independent of the length of the input. In the two-way case the dimension depends on the length of the input. Nevertheless, even in this case these matrices display a certain uniformity because they are tridiagonal block matrices where the blocks depend on the letters but have a fixed dimension independent of the length of the word.

I discussed the problem in June 2013 with Alberto at his place. He told me he had faced the same type of issue with Marcella Anselmo when working on two-way probabilistic automata. In a later work with Maria Paola Bianchi and Flavio d'Alessandro, [4] he used a clever result due L.G. Molinari: the varying dimension can be overcome by resorting to so-called *transfer matrices* which allow to work with matrices of a fixed dimension, [9]. The difficulty to apply the result is that we were working on a semiring $\mathrm{Rat}(\mathbb{N})$ of rational subsets of $\mathbb{N}$ and not on a ring, much less a field! We tried to work out a version which would suit better our poorer structure, unsuccessfully. Our final result was therefore obtained via completely different methods, but surprisingly the statement is formally pretty much the same. In the case of probabilistic automata, the probability of acceptance is given by the Hadamard quotient of two rational series with coefficients in the field of reals. More precisely, if w is the input, the probability of acceptance is equal to $p(w)/q(w)$, where $p(w)$ and $q(w)$ are the real coefficients of the term w in two $\mathbb{R}$-rational series. In our case the output of a two-way unary transducer is a finite sum of expressions of the form $p(w)q(w)^*$, where $p(w)$ and $q(w)$ are the coefficients of w in two $\mathrm{Rat}(\mathbb{N})$-rational series. There

E-mail address: cc@liafa.univ-paris-diderot.fr.
URL: http://www.liafa.jussieu.fr/~cc.

http://dx.doi.org/10.1016/j.tcs.2015.10.042
0304-3975/

are some differences between the two cases. For probabilistic automata, the input alphabet is finite but arbitrary. However, some assumptions of nonsingularity of the matrices are necessary. For transducers the result holds with the restriction that the input alphabet is unary, but makes no other assumption on the state transitions which is the equivalent of matrices in this case.

In order to state my result, I need some preliminaries. I will not recall the background on unary two-way transducers which is irrelevant in the present context. I assume the reader is familiar with the notion of rational subset of a monoid, here the additive monoid $\mathbb{N} \times \mathbb{N}$. A binary relation $R \subseteq \mathbb{N} \times \mathbb{N}$ can be viewed as a partial function from $\mathbb{N}$ into the powerset $\mathcal{P}(\mathbb{N})$ which allows us to write $R(n) = \{m \in \mathbb{N} \mid (n, m) \in R\}$ for all $n \in \mathbb{N}$. On the set of binary relations consider the operation which assigns $R^{\otimes}$ to R by setting $R^{\otimes}(n) = R(n)^*$ (this operation was introduced in [5] along with family of Hadamard relations). This paper inquires the condition under which a relation $R^{\otimes}$ is rational whenever R is rational. The main result is the following

Theorem 1.1. *Let $R \subseteq \mathbb{N} \times \mathbb{N}$ be a rational relation. The relation $R^{\otimes}$ is not rational if and only if there exist two integers $a \in \mathbb{N}, b \in \mathbb{N} \setminus \{0\}$ and $2p$ rational numbers $\alpha_1, \ldots, \alpha_p \in \mathbb{Q}, \beta_1, \ldots, \beta_p \in \mathbb{Q}_+ \setminus \{0\}$ such that the following holds*

$$R(n) = \bigcup_{i=1}^{p} (\alpha_i + \beta_i n) \quad \textit{for all } n \in a + b\mathbb{N}.$$

Furthermore, given a rational relation R it is decidable whether or not the relation $R^{\otimes}$ is rational.

For example, consider the rational relation $R = \{(n, n) \in \mathbb{N} \times \mathbb{N} \mid n \in \mathbb{N}\}$ which is the graph of the identity on $\mathbb{N}$. Then the relation $R^{\otimes} = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \text{ divides } m\}$ is not rational (this can be seen by observing that a rational relation is definable in the arithmetic with the addition only). A more elaborate example showing that it is necessary to allow rational and not only integer coefficients, is the following. Let R be defined for all $n \in 2 + 2\mathbb{N}$ as

$$R(n) = \{-1 + \frac{1}{2}n, -1 + n\}$$

(every input has two outputs). Then R is rational (a rational expression is $R = (2, 0) + (2, 1)^* \cup (2, 1) + (2, 2)^*)$ but $R^{\otimes}$ is not (a consequence of Corollary 4.3). Observe that the coefficients are rational numbers as in the statement of the Theorem.

I now relate the previous problem to a general problem on rational series. A $\mathbb{K}$-*series* on a variable x over a semiring $\mathbb{K}$ is a formal sum $s = \sum_{n \geq 0} s(n)x^n$. I assume the reader knows what it means for a series to be $\mathbb{K}$-*rational*. Consider a unary operation ω on $\mathbb{K}$ and extend it to the family of series by assigning to s the series s_ω defined by the condition $s_\omega(n) = \omega(s(n))$. If s is $\mathbb{K}$-rational, is it always the case that s_ω is also $\mathbb{K}$-rational? If the answer is no, determine under which condition it is or provide an algorithm to decide it. For example, Benzaghou characterized the rational series that are invertible in the Hadamard product, which is the special case where $\mathbb{K}$ is the field of reals and where ω is the operation of taking the multiplicative inverse in $\mathbb{K}$, see [2] or [10] for the same result with weaker hypotheses.

Now Theorem 1.1 can be interpreted in this general setting. Indeed, denote by $\text{Rat}(\mathbb{N})$ the semiring of the rational subsets of $\mathbb{N}$ where the addition and the product of the semiring are respectively the set union and the set addition. It can be proved that a binary relation $R \subseteq \mathbb{N} \times \mathbb{N}$ is rational if and only if the $\text{Rat}(\mathbb{N})$-series

$$s = \sum_{n \geq 0} R(n)x^n$$

is a $\text{Rat}(\mathbb{N})$-rational series. Define on $\text{Rat}(\mathbb{N})$ the operation that assigns $\omega(X) = X^*$ to $X \in \text{Rat}(\mathbb{N})$. Then the question I deal with can be translated as asking under which condition, for a $\text{Rat}(\mathbb{N})$-rational series s, the $\text{Rat}(\mathbb{N})$-series s_ω is also $\text{Rat}(\mathbb{N})$-rational.

The paper is organized as follows. Section 2 recalls the notion of series over a semiring, which extends that of series over a field along with the important family of rational series. The less classical notion of rational binary relations over the additive monoid of the nonnegative integers is also briefly reviewed. It is shown how relations and series may be thought of as one and the same object when properly interpreted. In particular the notion of Hadamard product is interpreted for binary relations (actually I speak of Hadamard sum rather than Hadamard product since the binary relations are additive structures) and we introduce the notion of Hadamard star, which is to Kleene star what the Hadamard product is to the product.

In Section 3 are concentrated the most technical aspects of this work. The idea is to obtain for an arbitrary subset of $\mathbb{N}$, an expression for the Kleene star in terms of the parameters defining the subset, as precisely as possible. However we do not deal with a single rational subset but more generally with the collection of subsets $R(n)$ when n ranges over the domain of definition of R. The objective is thus to compute the star uniformly, i.e., as a function of n. This is achieved thanks to a general formula giving an upper bound on the Frobenius number of a finite or infinite arithmetic progression of integers. Another ingredient is Eilenberg and Schützenberger's improvement, independently proved in [8], on previous results of Ginsburg and Spanier: indeed, the rational relations are *disjoint* unions (not merely unions) of "simple" rational relations. In Section 4 we apply their result and give a classification of these simple relations. It happens that these simple