An Hadamard operation on rational relations

Christian Choffrut

LIAFA, Université Paris Diderot - Paris 7 & CNRS, Case 7014 75205 Paris Cedex 13.

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.

Keywords: Finite automata, binary rational relations on integers, rational series, Hadamard product, Hadamard star, decidability.

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

Email address: cc@liafa.univ-paris-diderot.fr (Christian Choffrut)
URL: http://www.liafa.jussieu.fr/∼cc (Christian Choffrut)

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 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*

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

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 $\mathrm{Rat}(\mathbb{N})$ 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 $\mathrm{Rat}(\mathbb{N})$-series

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

is a $\mathrm{Rat}(\mathbb{N})$-rational series. Define on $\mathrm{Rat}(\mathbb{N})$ the operation that assigns $\omega(X) = X^*$ to $X \in \mathrm{Rat}(\mathbb{N})$. Then the question I deal with can be translated as asking under which condition, for a $\mathrm{Rat}(\mathbb{N})$-rational series s, the $\mathrm{Rat}(\mathbb{N})$-series s_ω is also $\mathrm{Rat}(\mathbb{N})$-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 relations have Hadamard stars which we are able to compute explicitly in Section 5. This allows us to give a proof of the theorem and to deliver a decision procedure.

2. Preliminaries

2.1. Rational series with coefficients in a semiring

Let $\mathbb{K}$ be a semiring provided with two binary operations of addition and product, respectively denoted $+$ and $\times$. The addition has a neutral element 0 and the multiplication has an identity element 1. It is assumed that all, possibly infinite, sums of elements of $\mathbb{K}$ are well-defined. In particular we assume that the unary operation $k \to k^* = \sum_{n\geq 0} k^n$ is well-defined.

A *series* is a function $s : \mathbb{N} \to \mathbb{K}$. (This is equivalent to the more classical definition as a formal sum of the form $\sum_{n\geq 0} s(n)x^n$ where x in an unknown). The elements of $\mathbb{K}$ are called *scalars* and $s(n)$ is the *coefficient* of n for the series s. The family of series over $\mathbb{K}$, denoted $\mathbb{K}\langle\langle\mathbb{N}\rangle\rangle$ is provided with the following operations where s, t represent two series and k a scalar:

- *multiplication by a scalar* $(s, k) \to ks$: $(ks)(n) = k \times s(n)$,
- *sum of series* $(s, t) \to s + t$: $(s + t)(n) = s(n) + t(n)$,
- *(Cauchy) product* $(s, t) \to s \times t$: $(s \times t)(n) = \displaystyle\sum_{n=n_1+n_2} s(n_1) \times t(n_2)$,
- *Kleene star*: $s \to s^*$: $(s^*)(n) = \displaystyle\sum_{n=n_1+\cdots+n_p, p\geq 0} s(n_1) \times \cdots \times s(n_p)$,
- *Hadamard product* (or H-product) $(s, t) \to s \odot t$: $(s \odot t)(n) = s(n) \times t(n)$,
- *Hadamard star* (or H-star): $s \to s^{\otimes}$: $s^{\otimes}(n) = (s(n))^*$.

The family of $\mathbb{K}$-*rational series* is the smallest family which contains the series having finite support (all but finitely many images equal to zero) and closed under scalar multiplication, sum, Cauchy product and Kleene star, see for example [3]. Furthermore, when the semiring is commutative the family of $\mathbb{K}$-rational series is closed under Hadamard product, e.g., [11, Thm III.3.1].

Proposition 2.1. *If $\mathbb{K}$ is commutative, the family of $\mathbb{K}$-rational series is closed under Hadamard product.*

2.2. Rational relations in an arbitrary monoid

The family of *rational* subsets of a monoid M denoted $\mathrm{Rat}(M)$, is the smallest family of subsets containing the finite subsets and closed under union, set product and Kleene star. Here we are mainly interested in the additive monoids $(\mathbb{N}, +, 0)$ and $(\mathbb{N} \times \mathbb{N}, +, (0,0))$. It is convenient to view elements of this latter structure as *vectors*. The operation is defined componentwise, i.e., $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. For obvious reasons, we comply to the usual terminology and prefer to speak of addition than product on these commutative structures.

We use the term *binary relation* or simply a *relation* for an arbitrary subset of the monoid $(\mathbb{N} \times \mathbb{N}, +, (0,0))$. Given two relations R and S we define the following operations which mimic those for the series.

- restriction to a subset $X \subseteq \mathbb{N}$: $R_X = R \cap (X \times \mathbb{N})$;
- union: $R, S \to R \cup S$;
- sum: $R, S \to R + S = \{(u_1 + v_1, u_2 + v_2) \mid (u_1, u_2) \in R, (v_1, v_2) \in S\}$;
- Kleene star:

$$R \to R^* = \{(u_1 + \cdots + u_n, v_1 + \cdots + v_n) \mid n \geq 0, (u_i, v_i) \in R\};$$

- *Hadamard sum* abbreviated *H-sum* (because the operation on the monoid is commutative I prefer to speak of Hadamard sum rather than Hadamard product): $R, S \to R \odot S = \{(u, v + w), \mid (u, v) \in R, (u, w) \in S\}$;
- *Hadamard star* (or H-star): $R \to R^{\otimes} = \{(u, v_1 + \cdots + v_n) \mid n \geq 0, (u, v_i) \in R\}$.

I refer to the literature for a thorough exposition of the theory, e.g., [6] and [11]. I content myself with recalling the basics. The family of rational subsets of an arbitrary monoid can be complex. For the monoid $\mathbb{N} \times \mathbb{N}$, it is a simple exercise to prove that they are precisely the relations which can be expressed as finite unions of *linear* relations, which are relations of the form

$$v_0 + v_1\mathbb{N} + \cdots + v_p\mathbb{N} \tag{1}$$

for some $p \in \mathbb{N}$ and where the v_i's belong to $\mathbb{N} \times \mathbb{N}$. Given a vector $v = (x, y)$ the notation $v\mathbb{N}$ represent the set $\{(nx, ny) \mid n \in \mathbb{N}\}$. Observe that $v\mathbb{N}$ is an alternative to the notation v^* showing thus these sets are indeed rational.

Example 2.2. *We have* $\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq n \leq m\} = (1,1)\mathbb{N} + (0,1)\mathbb{N}$ *and* $\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n = 2m\} = (2,1)\mathbb{N}$.

Given a relation $R \subseteq \mathbb{N} \times \mathbb{N}$ we denote by $\overline{R}$ the mapping of $\mathbb{N}$ into the power set $\mathcal{P}(\mathbb{N})$ defined for all integers $n \in \mathbb{N}$ by

$$\overline{R}(n) = \{m \mid (n, m) \in R\}.$$

We denote by $\mathrm{Dom}(\overline{R})$ the *domain* of R which is the set of integers n such that $\overline{R}(n) \neq \emptyset$. When R is a rational relation then $R(n) \in \mathrm{Rat}(\mathbb{N})$ and thus $\overline{R}$ is a $\mathrm{Rat}(\mathbb{N})$-series. However a stronger property holds since the family $\mathrm{Rat}(\mathbb{N} \times \mathbb{N})$ and the family of $\mathrm{Rat}(\mathbb{N})$-rational series can be identified [11, Proposition IV. 3.5.].

Proposition 2.3. *The mapping $R \mapsto \overline{R}$ defines a one-to-one correspondence between the family of rational relations and the family of* $\mathrm{Rat}(\mathbb{N})$*-rational series. Furthermore we have*

- $\overline{R \cup S} = \overline{R} + \overline{S}$,
- $\overline{R + S} = \overline{R} \times \overline{S}$,
- $\overline{R^*} = \overline{R}^*$,
- $\overline{R \odot S} = \overline{R} \odot \overline{S}$,
- $\overline{R^{\otimes}} = \overline{R}^{\otimes}$.

There is an important consequence of the above identification and of Proposition 2.1.

Proposition 2.4. *The family* $\mathrm{Rat}(\mathbb{N} \times \mathbb{N})$ *is closed under Hadamard sum.*

Consequently, deciding the closure of $\mathrm{Rat}(\mathbb{N} \times \mathbb{N})$ under the Hadamard star for binary relations, is equivalent to deciding the closure of the $\mathrm{Rat}(\mathbb{N})$-rational series under the Hadamard star for $\mathrm{Rat}(\mathbb{N})$-rational series.

Because of the above identification, from now on we will write $R(n)$ for $\overline{R}(n)$.

3. Kleene stars in Rat($\mathbb{N}$)

Due to the definition of the Hadamard star of a relation $R : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ that associates with every input the star of its image, it is natural to study as precisely as possible the star of a rational subset of $\mathbb{N}$. I start with the interplay between the three operations of Kleene star, set union and set sum. These properties rely heavily on the commutativity of the structure.

3.1. Elementary identities

Proposition 3.1. *With respect to the operation precedence: $* > + > \cup$ we have the following elementary identities for arbitrary subsets of* $\mathbb{N}$*:*

$$A^* + B^* = (A \cup B)^* \tag{2}$$

$$(A + B)^* = A^* + B^* \quad \text{if} \quad 0 \in A \cap B \tag{3}$$

$$(A + B^*)^* = \{0\} \cup A + A^* + B^* \quad \text{if} \quad 0 \notin A \tag{4}$$

Proof. Indeed, let us prove equality (2). The inclusion $A \subseteq A \cup B$ implies $A^* \subseteq (A \cup B)^*$. Similarly, we have $B^* \subseteq (A \cup B)^*$ and since $(A \cup B)^*$ is a submonoid, we get $A^* + B^* \subseteq (A \cup B)^*$. The inclusion from right to left is proved as follows. An element in $(A \cup B)^*$ is of the form $\sum_{0<i\leq n} c_i$ for some integer $n \geq 0$ where $c_i \in A \cup B$. By decomposing the subset $[0, n]$ into the index values for which $c_i \in A$ and those for which $c_i \in B$, and by taking advantage of the commutation, the element can be written as $\sum_{0<i\leq p} a_i + \sum_{0<j\leq q} b_i \in A^* + B^*$ with $a_i \in A$ and $b_j \in B$ and $p + q = n$.

Consider equality (3). Because $0 \in B$ we have $A \subseteq A + B$ and thus $A^* \subseteq (A + B)^*$. Similarly, we have $B^* \subseteq (A + B)^*$ and since $(A + B)^*$ is a submonoid this yields $A^* + B^* \subseteq (A + B)^*$. For the opposite direction it suffices to observe that an element in $(A + B)^*$ is of the form

$$\sum_{0<i\leq n} (a_i + b_i) = \sum_{0<i\leq n} a_i + \sum_{0<i\leq n} b_i \in A^* + B^*.$$

It remains to verify equality (4). The inclusion from left to right is a direct consequence of the expression of an arbitrary nonzero element in $(A + B^*)^*$, namely

$$\sum_{0<i\leq n} (a_i + b_i) = \sum_{0<i\leq n} a_i + \sum_{0<i\leq n} b_i = a_1 + \sum_{1<i\leq n} a_i + \sum_{0<i\leq n} b_i,$$

where $a_i \in A$ and $b_i \in B^*$. Now we prove the other inclusion. Since $0 \in B^*$ we have $A \subseteq A + B^*$ and thus $A^* \subseteq (A + B^*)^*$. Now $0 \in (A + B^*)^*$ and $A + B^* \subseteq (A + B^*)^*$. Because $(A + B^*)^*$ is a submomoid we have

$$\{0\} \cup A^* + (A + B^*) \subseteq (A + B^*)^*.$$

□

Observe that if $0 \notin A \cup B$ holds there is no interesting simplification of the expression.

3.2. Kleene star of an arithmetic progression

Here the purpose is, given a finite or infinite subset of positive integers to determine its Kleene star as exactly as possible. It is well-known that in $\mathbb{N}$ all infinite rational subsets have the finite power property, i.e., the star of an infinite rational subset $X \subseteq \mathbb{N}$ is the union of subsets of the form $\overbrace{X + \cdots + X}^{k \text{ operands}}$ over all integers k less than some given integer n, but it happens that in the case under study, we can explicitly give an upper bound for the number n as a function of the parameters defining the subset. The computation is tedious and based on a precise evaluation of the Frobenius number associated with an arithmetic progression.

Given a subset $I \subseteq \mathbb{N}$ of positive integers whose greatest common divisor equals 1, $G(I)$ denotes the greatest integer which does not belong to the submonoid generated by I, for instance $G(\{3, 5\}) = 7$. In the very special case of the

arithmetic progression with $\gcd(n,d)=1$ the closed formula can be simplified as follows, [1, p. 3]

$$G(n,n+d,\ldots,n+sd)=\lfloor\frac{n-2}{s}\rfloor n+d(n-1). \tag{5}$$

Let assume more generally that $\gcd(n,d)=p$ and observe that

$$G(n,n+d,\ldots,n+sd)=pG(\frac{n}{p},\frac{n+d}{p},\ldots,\frac{n+sd}{p})$$

holds. Then by the definition of G we get:

$$\{n,n+d,\ldots,n+sd\}^*\cap[G(n,n+d,\ldots,n+sd)+d,\infty[=p^*\setminus A,$$

where A is a subset of the interval $[0,G(n,n+d,\ldots,n+sd)]$.

Beyond the technical assertion of the next proposition, the point that should be remembered is the following: let n be the first element of an arithmetic progression with $\theta(n)$ elements. Then the Frobenius number is of order $\theta(n)$. It is clearly not the case when the progression has two elements (the classical case of the Frobenius number) and more generally when the number of elements is bounded, as can be shown using expression (5).

Proposition 3.2. *Let $a,b,d,p\in\mathbb{N}\setminus\{0\}$, $c\in\mathbb{Z}$, $p\in\mathbb{N}$ and $s=\lfloor\frac{bn+c}{a}\rfloor$. For some computable integer N, for all $n\geq N$ and $\gcd(n,d)=p$, it holds:*

$$G(n,n+d,\ldots,n+sd)\leq n(d+\left\lfloor\frac{a}{b}\right\rfloor+1)-d. \tag{6}$$

Let k be the unique integer satisfying $k\geq d+\lfloor\frac{a}{b}\rfloor+1>k-1$. Then

$$\{n,n+d,\ldots,n+sd\}^*=\bigcup_{0\leq i\leq k}\{n,n+d,\ldots,n+sd\}^i\ \cup nk+p\mathbb{N}. \tag{7}$$

Proof. The function $G(n,n+d,\ldots,n+sd)$ is nonincreasing in the variable s. The idea of the proof is to provide an upper bound for $\lfloor\frac{n-2}{s}\rfloor$ in (5). We abbreviate $G(n,n+d,\ldots,n+sd)$ as G.

Suppose a is a multiple of b, say $a=\lambda b$, i.e., $\lambda=\frac{a}{b}=\lfloor\frac{a}{b}\rfloor$. Then $s=\lfloor\frac{bn+c}{a}\rfloor=\lfloor\frac{n}{\lambda}+\frac{c}{a}\rfloor$. Setting $n=k\lambda+r$ with $0\leq r<\lambda$ we get $s=k+\lfloor\frac{c}{a}\rfloor+\epsilon_n$ with $\epsilon_n\in\{0,+1\}$. Assuming $k\geq-\frac{c}{a}+1$ so that $s>0$ we obtain

$$\frac{n-2}{s}=\frac{\lambda k+r-2}{k+\lfloor\frac{c}{a}\rfloor+\epsilon_n}.$$

Because of

$$0<\frac{\lambda k+r-2}{k+\lfloor\frac{c}{a}\rfloor+\epsilon_n}\leq\frac{\lambda k+\lambda-1}{k+\lfloor\frac{c}{a}\rfloor},$$

for $k\geq\lambda-1-(\lambda+1)\lfloor\frac{c}{a}\rfloor$ we have

$$\lambda k+\lambda-1\leq(\lambda+1)(k+\lfloor\frac{c}{a}\rfloor),$$

thus

$$0 < \left\lfloor \frac{n-2}{s} \right\rfloor \leq \left\lfloor \frac{\lambda k + \lambda - 1}{k + \left\lfloor \frac{c}{a} \right\rfloor} \right\rfloor \leq \frac{\lambda k + \lambda - 1}{k + \left\lfloor \frac{c}{a} \right\rfloor} \leq \lambda + 1.$$

Consequently, in this case we obtain

$$G \leq n(d + \left\lfloor \frac{a}{b} \right\rfloor + 1) - d.$$

Assume now a is not a multiple of b, set $n = ak + r$ with $0 \leq r < a$ and let

$$k > -\frac{1}{b} \left\lfloor \frac{c}{a} \right\rfloor.$$

We have

$$bn + c = b(ak + r) + c \geq bak + c \geq bak + a \left\lfloor \frac{c}{a} \right\rfloor > 0,$$

which implies $bn + c > 0$. Furthermore we get

$$\frac{bn + c}{a} \geq bk + \left\lfloor \frac{c}{a} \right\rfloor \text{ and thus } s = \left\lfloor \frac{bn + c}{a} \right\rfloor \geq bk + \left\lfloor \frac{c}{a} \right\rfloor.$$

Since $r < a$ this yields

$$\frac{n-2}{s} \leq \frac{ak + a - 2}{bk + \left\lfloor \frac{c}{a} \right\rfloor}.$$

We distinguish two cases. First, $a < b$. Then we have

$$\frac{ak + a - 2}{bk + \left\lfloor \frac{c}{a} \right\rfloor} < 1$$

whenever $k \geq \frac{a - 2 - \left\lfloor \frac{c}{a} \right\rfloor}{b - a}$ and therefore $\left\lfloor \frac{n-2}{s} \right\rfloor = 0$. This implies

$$G \leq (n-1)d = n(d + \left\lfloor \frac{a}{b} \right\rfloor) - d$$

which satifies condition . In the second case, we have $a > b$, i.e., $a = ub + v$ for some $0 < v < b$. A simple computation shows that we have

$$\frac{n-2}{s} < u + 1 \quad (= \left\lfloor \frac{a}{b} \right\rfloor + 1),$$

as soon as

$$k \geq \frac{a - 1 - (u+1) \left\lfloor \frac{c}{a} \right\rfloor}{b - v}$$

holds, which yields

$$G \leq n(\left\lfloor \frac{a}{b} \right\rfloor + d).$$

Therefore condition 3.2 is satisfied if furthermore $n \geq d$.

It remains to prove claim (7). By definition of G the left handside contains $nk + p\mathbb{N}$. Because n is the least element in $\{n, n + d, \ldots, n + sd\}$ and because $k \geq d + \left\lfloor \frac{a}{b} \right\rfloor$, all elements of the star less than or equal to kn are a sum of less than k elements in $\{n, n + d, \ldots, n + sd\}$.

□

By a suitable change of variable we have the following result, which is a special case of the Hadamard star of a rational relation.

Corollary 3.3. *Let $a, b, d, p, \lambda, \nu \in \mathbb{N} \setminus \{0\}$, $c \in \mathbb{Z}$, $\mu \in \mathbb{N}$ and $s = \lfloor \frac{bn+c}{a} \rfloor$. Consider the following rational subset of $\mathbb{N}$*

$$K = \{n \mid \lambda n + \mu \in \nu\mathbb{N} \text{ and } \gcd\big(\frac{\lambda n + \mu}{\nu}, d\big) = p\}.$$

Let k be the unique integer satisfying $k \geq d + \lfloor \frac{a\lambda}{\nu} \rfloor > k-1$. For some computable integer N and for all $n \in K$, with $n \geq N$ we have

$$\begin{aligned} & \{\frac{\lambda n+\mu}{\nu}, \frac{\lambda n+\mu}{\nu} + d, \ldots, \frac{\lambda n+\mu}{\nu} + sd\}^* \\ = & \bigcup_{0 \leq i \leq k} \{\frac{\lambda n+\mu}{\nu}, \frac{\lambda n+\mu}{\nu} + d, \ldots, \frac{\lambda n+\mu}{\nu} + sd\}^i \ \cup \frac{\lambda n+\mu}{\nu} k + p\mathbb{N}. \end{aligned} \tag{8}$$

4. Rational relations

The following computations lead to natural expressions which do not completely respect the definition of linear sets as given in (1) but which may be proven equivalent. We explain this on an example. Consider the following expression

$$(-\frac{5}{2}, 0) + (1, \frac{1}{3})\mathbb{N} + (\frac{1}{2}, 1)\mathbb{N} = \{(-\frac{5}{2} + x + \frac{1}{2}y, \frac{1}{3}x + y) \mid x, y \in \mathbb{N}\} \tag{9}$$

and assume that we are interested in the subset of vectors with nonnegative integer components. On this example I use modular arithmetic but I will not do it explicitly in the sequel. Indeed, if an element of the above set has integer components then $x = 0 \bmod 3$, $y = 1 \bmod 2$. Consider the change of variable: $x = 3x'$ and $y = 1 + 2y'$. We obtain the set

$$\{(-1 + 3x' + y', x' + 2y') \mid x', y' \in \mathbb{N}\}.$$

Since this set contains elements whose components are negative, we must impose $x' \geq 1$ or $y' \geq 1$. The latter condition leads to the change of variable $x' = x'' + 1$ and to the expression

$$(2, 1) + (3, 1)\mathbb{N} + (1, 2)\mathbb{N} \tag{10}$$

and the former condition leads to the change of variables $y' = y'' + 1$ and to the expression

$$(0, 2) + (3, 1)\mathbb{N} + (1, 2)\mathbb{N}. \tag{11}$$

Consequently, expression (9) is equivalent on $\mathbb{N} \times \mathbb{N}$ to the union of expressions (10) and (11).

4.1. Decomposition of rational relations

In order to simplify the computations we use a more precise definition than that given in (1), which is independently due to [6] and to [8], see also [11] for example. Indeed, call *simple* a subset of $\mathbb{N} \times \mathbb{N}$ defined as in (1) with the additional condition that the v_i's are linearly independent which implies in particular $p \leq 2$. Then the family of rational relations is exactly the family of finite unions of disjoint simple relations. I state the result for binary relations but it holds for relations of arbitrary arity.

Theorem 4.1 ([6])**.** *A binary rational relation in $\mathbb{N} \times \mathbb{N}$ is a finite disjoint union of relations which are the nonnegative solutions in the variables n and t of systems of the following form*

$$\left.\begin{array}{l} n = a_1 + b_1 x + c_1 y \\ t = a_2 + b_2 x + c_2 y \end{array}\right\} \quad a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{N} \tag{12}$$

when x and y run over $\mathbb{N}$, subject to the condition that the vectors (b_1, b_2) and (c_1, c_2) are linearly independent.

Eilenberg and Schützenberger use the term *simple* for the relations satisfying (12). This improvement on the definition given in (1) facilitates the computations greatly.

So from now on and unless otherwise stated, we deal with relations defined by systems of the form 12. When working with general results, i.e., with finite unions of the latter relations, we will say it explicitly.

4.2. Simple rational relations

The purpose is to eliminate the parameters x and y in (12) in order to express t as a function of n. We first investigate the case where the relation R is defined by a unique system (12). Observe that the condition on the vectors (b_1, b_2) and (c_1, c_2) is equivalent to

$$b_1 c_2 - b_2 c_1 = 0 \Rightarrow b_1 = b_2 = 0 \text{ or } c_1 = c_2 = 0. \tag{13}$$

Proposition 4.2. *There are five different types of simple relations determined by the solutions of the system (12). The domain of definition and an expression are given below for each type of relation.*

Type 1*: $b_1 = c_1 = 0$. Then $R = (a_1, a_2) + (0, b_2)\mathbb{N} + (0, c_2)\mathbb{N}$, i.e., for all $n \in Dom(R) = \{a_1\}$ it holds*

$$R(n) = a_2 + b_2\mathbb{N} + c_2\mathbb{N}. \tag{14}$$

Type 2*: $b_1 \neq 0, b_2 = c_1 = 0$. Then $R = (a_1, a_2) + (b_1, 0)\mathbb{N} + (0, c_2)\mathbb{N}$, i.e., for all $n \in \mathrm{Dom}(R) = a_1 + b_1\mathbb{N}$ it holds*

$$R(n) = a_2 + c_2\mathbb{N}. \tag{15}$$

Type 3*:* $b_1, b_2 \neq 0, c_1 = c_2 = 0$*. Then* $R = (a_1, a_2) + (b_1, b_2)\mathbb{N}$*, i.e., for all* $n \in \mathrm{Dom}(R) = a_1 + b_1\mathbb{N}$ *it holds*

$$R(n) = a_2 + b_2 \frac{n - a_1}{b_1}. \tag{16}$$

Type 4*:* $b_1, b_2, c_2 \neq 0, c_1 = 0$*. Then* $R = (a_1, a_2) + (b_1, b_2)\mathbb{N} + (0, c_2)\mathbb{N}$*, i.e., for all* $n \in \mathrm{Dom}(R) = a_1 + b_1\mathbb{N}$ *it holds*

$$R(n) = a_2 + b_2 \frac{n - a_1}{b_1} + c_2\mathbb{N}. \tag{17}$$

Type 5*:* $b_1, b_2, c_1, c_2 \neq 0$*, and thus* $b_1c_2 - b_2c_1 \neq 0$ *by condition 13. Define*

- *the values*
$$A = a_2b_1 - a_1b_2, B = c_2b_1 - c_1b_2, \tag{18}$$
- *the predicate*
$$P(\alpha, \beta) \equiv \alpha - a_1 - c_1\beta = 0 \bmod b_1 \text{ and } 0 \leq \alpha, \beta < b_1. \tag{19}$$

For all $0 \leq \alpha < b_1$ *consider the rational subset* $K_\alpha = \alpha + b_1\mathbb{N} \cap (a_1 + \mathbb{N})$ *and denote by* R_α *the restriction of* R *to* K_α*. Then* $\mathrm{Dom}(R) = \bigcup_{0 \leq \alpha < b_1} K_\alpha$*. Furthermore, we have* $R_\alpha = \bigcup_{P(\alpha,\beta)} R_{\alpha,\beta}$ *where for an effectively computable* $N_{\alpha,\beta}$ *and for all integers* $n \geq N_{\alpha,\beta}$ *we have*

$$R_{\alpha,\beta}(n) = \frac{(A + b_2n + \beta B)}{b_1} + B\{0, \ldots, \left\lfloor \frac{n - a_1 - \beta c_1}{b_1c_1} \right\rfloor\}. \tag{20}$$

Proof. We omit the verification of the first four types which is routine. For the last type, by substituting $\frac{n - a_1 - c_1y}{b_1}$ for x in the expression of t we get the following conditions on the solutions

$$\begin{aligned} &b_1t = A + b_2n + By, \\ &n - a_1 - c_1y \geq 0. \end{aligned} \tag{21}$$

Since x is an integer we have the other condition

$$n - a_1 - c_1y = 0 \qquad \bmod b_1. \tag{22}$$

We fix a value modulo b_1 for the variables n and y, resp. α and β which must satisfy the predicate (19).

We proceed to a case study depending on the signs of the parameters A and B. Observe that under our assumption on α and β the value of t in (21) is always an integer.

Case 1: $A \geq 0, B \geq 0$. The solutions for t are positive whatever the value of n and the only remaining condition (21) can be rewritten as

$$0 \leq y \leq \frac{n - a_1}{c_1}. \tag{23}$$

Case 2: $A < 0, B \geq 0$. The condition on y under which t is nonnegative is

$$\max\{0, \frac{-A - b_2 n}{B}\} \leq y \leq \frac{n - a_1}{c_1}.$$

For $n \geq \frac{-A}{b_2}$ the maximum term to the left is 0 and the condition reduces to (23). Whatever the value of n, the number of possible values for y is finite.

Case 3: $A \geq 0, B < 0$. The condition on y under which t is nonnegative is

$$0 \leq y \leq \min\{\frac{-A - b_2 n}{B}, \frac{n - a_1}{c_1}\}.$$

If $n > \frac{a_1 c_2 - a_2 c_1}{c_2}$ holds, we have $\frac{n-a_1}{c_1} \leq \frac{-A-b_2 n}{B}$ and therefore the condition reduces to (23). Whatever the value of n, the number of possible values for y is finite.

Case 4: $A < 0, B < 0$. The conditions on y under which t is nonnegative is

$$0 \leq y \leq \min\{\frac{-A - b_2 n}{B}, \frac{n - a_1}{c_1}\}.$$

For $n \geq \frac{a_1 c_2 - a_2 c_1}{c_2}$ the minimum of the right expression of the condition is $\frac{n-a_1}{c_1}$ and the condition reduces to (23). Whatever the value of n, the number of possible values for y is finite.

Consequently, in all these four cases, provided n is sufficiently large, inequality (23) is the unique condition on y. Now we assumed $y = \beta \bmod b_1$, i.e., $y = \beta + k b_1$ for some integer k. The condition (23) is thus equivalent to

$$y = \beta + k b_1, \text{ with } k = 0, \ldots, \lfloor \frac{n - a_1 - \beta c_1}{b_1 c_1} \rfloor$$

which provides expression (20).

□

4.3. A necessary condition for rationality for binary relations

We recall that an infinite subset $X \subseteq \mathbb{N}$ is rational if and only if there exist two integers t, p and two subsets $A \subseteq [0, t[$, $B \subseteq [0, p[$ such that $X = A \cup t + B + p\mathbb{N}$ holds. The integers p, t and the subset B can be made unique (in that case p is called the *ultimate period* of X) but I will not need this refinement. The next result states a necessary condition for a binary relation to be rational. Intuitively it says that for all inputs with a finite image, the maximum element

in the image is linearly bounded by the input, and for all inputs with an infinite image the above integer t is linearly bounded by the input and the integer p is one of finitely many different values. E.g., with these criteria, the following relations are not rational

$$R_1(n) = n\mathbb{N},\ R_2(n) = n^2 + \mathbb{N}.$$

Lemma 4.3. *If R is a binary rational relation there exists a finite subset $P \subseteq \mathbb{N}$ such that for all integers n we have:*

- *if $R(n)$ is finite then $\max R(n) = O(n)$;*
- *if $R(n)$ is infinite then it is of the form $A(n) \cup t(n) + B + p\mathbb{N}$ with $A(n) \subseteq [0, t(n)[$, $B \subseteq [0, p[$, $t(n) = O(n)$ and $p \in P$.*

Proof. The claim holds for simple relations. Indeed, this is obvious for type 1, 2, 3 and 4 because of the expressions (14), (15), (16) and (17). For type 5, expression (20) holds for all possible values α and β satifying (19) and for all sufficiently large n. For all other (finitely many) values of n, the image is finite.

Assume now that we have a finite union of such simple relations, say $R = R_1 \cup \cdots \cup R_k$. The coarsest refinement of their domain of definition is a finite disjoint union of rational subsets of $\mathbb{N}$. It suffices to consider the restrictions of the relations on one of these relations. In other words, there is no loss of generality to assume that the relations have the same domain of definition. If $R(n)$ is finite so is every $R_i(n)$ for $i = 1, \ldots, k$. Now $\max R_i = O(n)$ for $i = 1, \ldots, k$ implies $\max R = \max(R_1 \cup \cdots \cup R_k) = O(n)$.

Assume now the set I of indices $i \in \{1, \ldots, k\}$ such that $R_i(n)$ is infinite is nonempty. For each $i \in I$, we have

$$R_i(n) = A_i(n) \cup (t_i(n) + B_i + p_i\mathbb{N})$$

with $A_i(n) \subseteq [0, t_i(n)[$, $t_i(n) = O(n)$, $B_i \subseteq [0, p_i[$ and $p_i \in P_i$. Observe that for all $t(n) \geq t_i(n)$ there exist $A'_i(n) \subseteq [0, t(n)[$ and $B'_i \subseteq [0, p_i[$ such that the following holds

$$A_i(n) \cup (t_i(n) + B_i + p_i\mathbb{N}) = A'_i(n) \cup (t(n) + B'_i + p_i\mathbb{N}), \tag{24}$$

with $t_i(n) + B_i = t(n) + B'_i \bmod p_i$ where B'_i depends on the value of $t(n)$ modulo p_i. It suffices to prove that for a fixed value of n modulo p_i, $i \in I$ the expression of $R(n)$ is of the right form. Pose $\tau(n) = \max\{t_i(n) \mid i \in I\}$ and observe that $\tau(n) = O(n)$. Take the union of the R_i's for $i \in I$ and apply (24). We get

$$R(n) = A(n) \cup \bigcup_{i \in I} (\tau(n) + B'_i + p_i\mathbb{N}) = A(n) \cup \tau(n) + \bigcup_{i \in I} (B'_i + p_i\mathbb{N})$$

with $A(n) \subseteq [0, \tau(n)[$ and $B'_i \subseteq [0, p_i[$. The subset $\bigcup_{i \in I}(B'_i + p_i\mathbb{N})$ is rational and its ultimate period p divides the least common multiple of the p_i's. Therefore

for some integer s, some $A' \subseteq [0, s[$ and some $B \subseteq [0, p[$ we have $\bigcup_{i \in I}(B'_i + p_i\mathbb{N}) = A'(n) \cup s + B + p\mathbb{N}$. Finally, we have

$$R(n) = (A(n) \cup \tau(n) + A'(n)) \cup \tau(n) + s + B + p\mathbb{N}$$

i.e., $R(n) = C(n) \cup \theta(n) + B + p\mathbb{N}$ with $\theta(n) = \tau(n) + s$ and $C(n) = A(n) \cup \tau(n) + A'(n)$.

□

Observe also that the condition is not sufficient: consider the characteristic function of any non recursive function from $\mathbb{N}$ to $\mathbb{N}$.

5. Hadamard star of rational relations

5.1. A particular case of the Hadamard sum

The following result plays a crucial role in the correctness proof of the procedure. It states a general result under which the Hadamard sum of a rational and a nonrational relation is rational. Intuitively, the reason is that the rational relation "covers" or "hides" almost all of the nonrational relation. In the next result recall the discussion at the beginning of Section 4 concerning the use of rational, noninteger coefficients.

Lemma 5.1. *Let X be a rational subset of $\mathbb{N}$ and let $R_1, R_2 \subseteq \mathbb{N} \times \mathbb{N}$ satisfy the following conditions for all $n \in X$*

$$\begin{array}{ll} R_1(n) = A(n) + c\mathbb{N} & c \in \mathbb{N} \setminus \{0\}, A(n) \text{ a finite subset of } \mathbb{N}, \\ R_2(n) = (a + bn)\mathbb{N} & a \in \mathbb{Q}, b \in \mathbb{Q}_+. \end{array}$$

If R_1 is rational, so is the restriction of $R_1 \odot R_2$ to X.

Proof. Equality $\mathbb{N} = \bigcup_{0 \le i < c} c\mathbb{N} + i$ holds. Furthermore by applying the identity $A(B + C_1 \cup B + C_2) = AB + (AC_1 \cup AC_2)$ where A, B, C_1, C_2 are subsets of $\mathbb{N}$, the set $(a + bn)\mathbb{N}$ is equal to

$$(a + bn)\Big(\bigcup_{0 \le i < c} c\mathbb{N} + i\Big) = (a + bn)c\mathbb{N} + \bigcup_{0 \le i < c} (a + bn)i.$$

Since $a + bn$ is an integer whenever it belongs to X we have

$$(a + bn)c\mathbb{N} = c((a + bn)\mathbb{N}) \subseteq c\mathbb{N}.$$

Finally we get

$$R_1(n) + R_2(n) = A(n) + c\mathbb{N} + \{0, a + bn, \ldots, (a + bn)(c - 1)\}.$$

The relation S defined by $S(n) = a + bn$ for all $n \in X$ is clearly rational and so are all Hadamard sums of the form $S^{(i)} = S \overbrace{\odot \cdots \odot}^{i \text{ operands}} S$ with the convention $S^{(0)}(n) = \{0\}$. For all $n \in X$ we have

$$(R_1 + R_2)(n) = \bigcup_{0 \leq i < c} (R_1(n) + S^{(i)}(n))$$

and we may conclude by the closure properties of rational relations under union and Hadamard sum.

□

Proposition 5.2. *Let R be a simple relation. Then for all $n \notin \mathrm{Dom}(R)$ we have $R^{\otimes}(n) = \{0\}$. For all $n \in \mathrm{Dom}(R)$, the following determines their image in the Hadamard star for the five types of relations in the classification of Proposition 4.2. For all except type 3, the Hadamard star is rational.*

Type 1*: $b_1 = c_1 = 0$. For all $n \in Dom(R)$ we have*

$$R^{\otimes}(n) = \{0\} \cup a_2 + a_2\mathbb{N} + b_2\mathbb{N} + c_2\mathbb{N}.$$

Type 2*: $b_1 \neq 0, b_2 = c_1 = 0$. For all $n \in \mathrm{Dom}(R)$ we have*

$$R^{\otimes}(n) = \{0\} \cup a_2 + a_2\mathbb{N} + c_2\mathbb{N}.$$

Type 3*: $b_1, b_2 \neq 0, c_1 = c_2 = 0$. For all $n \in \mathrm{Dom}(R)$ we have*

$$R^{\otimes}(n) = (a_2 + b_2\frac{n - a_1}{b_1})^*. \tag{25}$$

Type 4*: $b_1, b_2, c_2 \neq 0, c_1 = 0$. For all $n \in \mathrm{Dom}(R)$ we have*

$$R^{\otimes}(n) = \{0\} \cup \bigcup_{0 \leq r < c_2} (a_2 + \frac{n - a_1}{b_1} b_2)(r + 1) + c_2\mathbb{N}. \tag{26}$$

Type 5*: $b_1, c_1, b_2, c_2 \neq 0$. Let α, β satisfy condition 19 in Proposition 4.2 and observe that the values are less than or equal to b_1. Let p_β be the greatest common divisor of $\frac{(A + b_2 n + \beta B)}{b_1}$ and B. Observe that it depends on α and not on n. Then for some computable k_β and for all integers $n \geq N_{\alpha,\beta}$ we have*

$$\begin{aligned} R^{\otimes}_{\alpha,\beta}(n) = \bigcup_{0 \leq i < k_\beta} \{\frac{(A + b_2 n + \beta B)}{b_1} + B\{0, \ldots, \left\lfloor \frac{n - a_1 - \beta c_1}{|B|} \right\rfloor\}^i \\ \cup (\frac{(A + b_2 n + \beta B)}{b_1} k_\beta + p_\beta\mathbb{N}. \end{aligned} \tag{27}$$

Proof. The verification of the expression of the Hadamard star for the first four types is routine. It is clear that for the first two types this expression is rational. Type 3 is not rational because of Lemma 4.3. The expression and the rationality for type 4 are direct consequences of Lemma 5.1.The assertion concerning type 5 is a consequence of the following claim.

Claim. With the same hypotheses as Corollary 3.3 the Hadamard star of the rational relation

$$\{(n, \{\frac{\lambda n+\mu}{\nu}, \frac{\lambda n+\mu}{\nu}+d, \ldots, \frac{\lambda n+\mu}{\nu}+sd\}) \mid n \in K\}$$

is rational.

Indeed, for sufficiently large n, we apply Corollary 3.3. The first term of the union is a finite union of powers of the rational relation

$$\{(n, \{\frac{\lambda n+\mu}{\nu}, \frac{\lambda n+\mu}{\nu}+d, \ldots, \frac{\lambda n+\mu}{\nu}+sd\}) \mid n \in K\}.$$

The second term of the union is the restriction to K of the relation

$$\frac{1}{\nu}[(\nu, \lambda)^* + (0, \mu)] + K \times p\mathbb{N}.$$

□

5.2. Hadamard star of general rational relations

The first result is an immediate consequence of Equation 2.

Lemma 5.3. *For all relations $(R_i)_{i=1,\ldots,k}$ we have*

$$\big(\bigcup_{i=1}^{k} R_i\big)^{\otimes} = \sum_{i=1}^{k} R_i^{\otimes}. \tag{28}$$

Each rational relation is a finite union of simple relations of type 1 up to 5. If none of these relations is of type 3, by Lemma 5.3 the Hadamard star of the union is rational.

Corollary 5.4. *Let $(R_i)_{i=1,\ldots,k}$ be a family of simple relations of type 1,2,4 or 5. Then $\big(\bigcup_{i=1}^{k} R_i\big)^{\otimes}$ is rational*

Now we investigate the case where all of the simple relations are of type 3.

Lemma 5.5. *Let $(R_i)_{i=1,\ldots,k}$ be a family of type 3 simple relations with the same infinite domain of definition. Then $\big(\bigcup_{i=1}^{k} R_i\big)^{\otimes}$ is not rational.*

Proof. There exists an infinite rational subset X of the form $\alpha + \beta\mathbb{N}$ for some $\alpha \in \mathbb{N}$ and $\beta \in \mathbb{N} \setminus \{0\}$ in the common domain of definition of the relations. We

consider the restrictions of the relations to X. Each relation is of the form (25). By reducing them to the same denominator d we have

$$\text{for all } n \in X: \quad (R(n))^* = \frac{1}{d}\sum_{i=1}^{k}(nc_i + e_i)^* \ . \tag{29}$$

If the vectors $(c_i, e_i) \in \mathbb{N}\times\mathbb{N}$ are collinear then for some vector $(c, e) \in \mathbb{Q}_+ \times \mathbb{Q}_+$ we have $(c_i, e_i) = k_i(c, e)$ with $k_i \in \mathbb{N}$. Hence,

$$\sum_{i\in I}(nc_i + e_i)^* = \sum_{i\in I}(k_i(nc + e))^* = (nc + e)\sum_{i\in I} k_i^* = (nc + e)\{k_1, \ldots, k_n\})^*.$$

Let p be the gcd of the k_i's. Then the ultimate period of the images of the elements in the restriction of R to X is $p(nc + e)$. Since $n \in \alpha + \beta\mathbb{N}$ holds, the set of ultimate periods $\{p(\alpha + \beta x) + e \mid x \in \mathbb{N}\}$ is infinite and the restriction cannot be rational by Lemma 4.3.

If there are two noncollinear vectors, say without loss of generality (c_1, e_1) and (c_2, e_2), for all integers n the greatest common divisor of $nc_1 + e_1$ and $nc_2 + e_2$ divides the integer $c_1e_2 - c_2e_1$. Therefore for a fixed integer n, the greatest common divisor p of all $nc_i + e_i$ is again a divisor of $c_1e_2 - c_2e_1$ and thus assumes only finitely many possible values. By [7] cited in [1, Thm 3.6.4] for all expressions $A \cup t + p\mathbb{N}$ with $A \subseteq [0, t[$ defining the submonoid 29 we have $t = \Omega(n^{\frac{k}{k-1}})$, a contradiction with the conclusion of Lemma 4.3. □

There remains to consider the case where the union contains a simple relation of type 3 and some simple relation of a different type.

Lemma 5.6. *Let $T = \bigcup_{i=1}^{k} R_i$ be union of k simple relations having the same domain of definition. Assume that R_1 is of type 1,2,4 or 5 and that for $i = 2, \ldots, k$, R_i is of type 3. Then the restriction of $T^{\otimes}$ to X is rational.*

Proof. For all $n \in X$ we have

$$T^{\otimes}(n) = R_1(n)^* + \sum_{i=2}^{k} R_i(n)^* = \sum_{i=2}^{k}(R_1(n)^* + R_i(n)^*).$$

Thus, by the closure property of rational relations under Hadamard sum, it suffices to consider the special case where $k = 2$, i.e., R_1 is of type 1,2,4 or 5 and R_2 is of type 3. The case of type 1 is trivial since under these conditions X is a singleton. For types 2, 4 and 5 this is a consequence of Lemma 5.1.

□

5.3. The proof of Theorem 1.1

We now turn to the proof of the theorem and show that it is effective.

Proof of Theorem 1.1. We are given a rational relation R by a finite number of systems Σ_i, $i = 1, \ldots, k$, of the form (12) each defining a relation R_i. Consider the coarsest refinement of the domains of definition of the R_i's, say $\mathbb{N} = \bigcup_k X_k$, which is a union of disjoint rational subsets of $\mathbb{N}$. Now $R^{\otimes}$ is not rational if and only if there exists some X_k such that the Hadamard star of the restriction of R to X_k is not rational. By Corollary 5.4 and Lemmas 5.5 and 5.6 this is equivalent to say that there exists some infinite X_k for which all relations R_i defined on X_k are of type 3. This is again equivalent to the following: let I be the set of indices i such that X_k is included in the domain of definition of R_i. Then for some infinite subset $a + b\mathbb{N} \subseteq X_k$ there exist $\alpha_i, \beta_i, i \in I$, $\alpha_i \in \mathbb{Q}, \beta_i \in \mathbb{Q}_+$ such that $R_i(n) = \alpha_i + \beta_i n$, i.e.,

$$R(n) = \bigcup_{i=1}^{p} R_i(n) = \bigcup_{i \in I} R_i(n) = \bigcup_{i \in I} \alpha_i + \beta_i n.$$

Finally let us observe that the proof can be converted into an algorithm. Indeed, the above discussion can be reformulated as follows. For each binary relation R_i defined by the system Σ_i, its domain of definition along with its type can be explicitly computed, see Lemma 4.2. Let Y be the union of the domains of definition of the relations of type 3 and let Z be the union of the domains of definition of the relations of type different from 3. Then the Hadamard inverse of R is rational if and only if $Y \setminus Z$ is finite. Since both Y and Z are rational subset, this condition is decidable. □

5.4. Complexity

The complexity of the algorithm deciding whether or not the Hadamard inverse of a rational relation R is rational depends on the way R is given. We assume R is defined by k systems of equations as in (12) where all integers are expressed in binary. Let C be the maximum length of the representations of the constants such as a_1, a_2 in (12) and let P be the maximum length of the representations of the other coefficients such as b_1, b_2, c_1, c_2 in (12). We shall bound the complexity as a function of k, C and P.

We start with an operation whose objective is to reduce the impact of too large values of constants in the construction of finite automata as alluded above. This is also why we separated the constants from the other coefficients. Consider an infinite rational subset of the form

$$X = A \cup t + B + p\mathbb{N}, A \subseteq [0, t-1], B \subseteq [0, p-1],$$

where p and t are minimal (this is the natural expression associated with the minimal automaton recognizing X). We assign to X the rational subset

$$\Gamma(X) = p\mathbb{N} + ((t + B) \bmod p).$$

The notation $z \bmod p$, extended to subsets in a natural way, represents the unique integer in the interval $[0, p-1]$ which is equal to z modulo p. E.g., with the set $X = \{1,4\} \cup 17 + \{1,3\} + 5\mathbb{N}$ we have $\Gamma(X) = \{0,3\} + 5\mathbb{N}$. Observe that for all $x \geq t$ we have $x \in X \Leftrightarrow x \in \Gamma(X)$. Indeed, $x \geq t, x \in X$ implies $x = t+b+kp$ for some $k \geq 0$ and some $b \in B$. Then dividing $t+b$ by p leads us to equality $t + b = \ell p + b'$ and therefore $x = (\ell + k)p + b' \in \Gamma(X)$. Conversely, if $x \in \Gamma(X)$ then $x = pu + (t + b) - pv$ for some $b \in B$ and some $u, v \in \mathbb{N}$ where $pv \leq t + b < p(v + 1)$. If $x \geq t$ we have furthermore $u - v \geq 0$, i.e., $x = t + b + (u - v)p \in X$. The purpose of the notation $\Gamma(X)$ is to simplify the coefficients of the rational expression without modifying too much the subset and to bound the size of the minimal automaton to p. Indeed, with the previous discussion we have

$$X \setminus Y \text{ is finite } \Leftrightarrow \Gamma(X) \setminus \Gamma(Y) \text{ is finite.}$$

Proposition 5.7. *Let R be a rational relations given as in the beginning of tis subsection 5.4.*

It is decidable in time $O(kC + 2^{kP})$ whether or not the Hadamard inverse of R is rational.

Proof. Indeed, by a simple inspection on the coefficients we sort out the k systems as $k' \leq k$ systems defining simple relations of type different from 3, say $R_1, \ldots, R_{k'}$ and the $k - k'$ other systems. By the claim at the end of the proof of Theorem 1.1, it suffices to decide whether or not the subset

$$\bigcup_{i=k'+1}^{k} \mathrm{Dom}(R_i) \setminus \bigcup_{j=1}^{k'} \mathrm{Dom}(R_j) = \bigcup_{i=k'+1}^{k} \mathrm{Dom}(R_i) \cap \bigcap_{j=1}^{k'} (\mathbb{N} \setminus \mathrm{Dom}(R_j))$$

is finite, which is equivalent to decide whether or not the subset

$$\bigcup_{i=k'+1}^{k} \Gamma(\mathrm{Dom}(R_i)) \cap \bigcap_{j=1}^{k'} (\mathbb{N} \setminus \Gamma(\mathrm{Dom}(R_j)))$$

is finite. This is achieved by constructing the finite automaton that is the direct product of the k minimal automata for all $\Gamma(\mathrm{Dom}(R_i)), i = 1, \ldots, k$. If $\mathrm{Dom}(R_i) = a + b\mathbb{N}$ then the minimal automaton for $\Gamma(\mathrm{Dom}(R_i))$ has b states and if $\mathrm{Dom}(R_i) = a + b\mathbb{N} + c\mathbb{N}$ the minimal automaton for $\Gamma(\mathrm{Dom}(R_i))$ has $\gcd(b, c)$ states, i.e., in both cases it has $O(2^P)$ states, thus the overall construction has complexity $O((2^P)^k) = O(2^{kP})$ because computing the greatest common divisor of two integers is linear in the representations of the integers.

Now we need to determine the type to which each R_i belongs. This is done by a simple inspection of the coefficients a_i, b_i, c_i, $i = 1, \ldots, k$. Finally, in order to construct the minimal automata $\Gamma(\mathrm{Dom}(R_i))$ we consider two cases. If $\mathrm{Dom}(R_i)$ is of the form $a + b\mathbb{N}$ it suffices to compute the remainder of the division of a by b. Otherwise, if it is of the form $a + b\mathbb{N} + c\mathbb{N}$ it suffices to compute the remainder of a in the division of a by $d = \gcd(b, c)$. These k last computations have complexity $O(kC)$. □

[1] J. L. Ramírez Alfonsín. *The Diophantine Frobenius Problem*. Number 30 in Oxford Lecture series in mathematics. Oxford University Press, 2005.

[2] B. Benzaghou. Algèbres de Hadamard. *Bulletin de la Société Mathématique de France*, 98:209–252, 1970.

[3] J. Berstel and C. Reutenauer. *Rational series and their languages*, volume 12. Springer-Verlag, 1988.

[4] A. Bertoni, M.-P. Bianchi, and F. D'Alessandro. Regularity of languages defined by formal series with isolated cut point. *RAIRO - Theor. Inf. and Applic.*, 46(4):479–493, 2012.

[5] C. Choffrut and B. Guillon. An algebraic characterization of unary two-way transducers. In *Proceedings of the 15th Italian Conference on Theoretical Computer Science, Perugia, Italy, September 17-19, 2014.*, pages 279–283, 2014.

[6] S. Eilenberg and M.-P. Schützenbeger. Rational sets in commutative monoids. *Journal of Algebra*, 13(2):173–191, 1969.

[7] M. Hujter. On a sharp upper and lower bounds for the Frobenius problem. Technical Report MO 32, Hungarian Academy of Sciences, 1982.

[8] R. Ito. Every semilinear set is a finite union of disjoint linear sets. *J. Comput. Syst. Sci.*, 3(2):221–231, 1969.

[9] L. G. Molinari. Determinants of block tridiagonal matrices. *Linear Algebra Appl.*, 429(8–9):2221–2226, 2008.

[10] C. Reutenauer. Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles. *Bulletin de la Société Mathématique de France*, 110:225–232, 1982.

[11] J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.